(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
12 September 2002 (12.09.2002)

PCT

(10) International Publication Number
WO 02/071224 A1

(51) International Patent Classification[7]: G06F 11/30, 12/00, 12/14, 12/16, 13/00, 13/28, 15/16, 15/173, H04L 9/00, 9/32

(21) International Application Number: PCT/IL02/00152

(22) International Filing Date: 27 February 2002 (27.02.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/272,389 1 March 2001 (01.03.2001) US

(71) Applicant *(for all designated States except US)*: STORAGE NETWORKING TECHNOLOGIES [IL/IL]; 63 Bar Yehuda Str., 36651 Nesher (IL).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: NAHUM, Nelson [IL/IL]; 4 Morad Hayasmin, 34762 Haifa (IL).

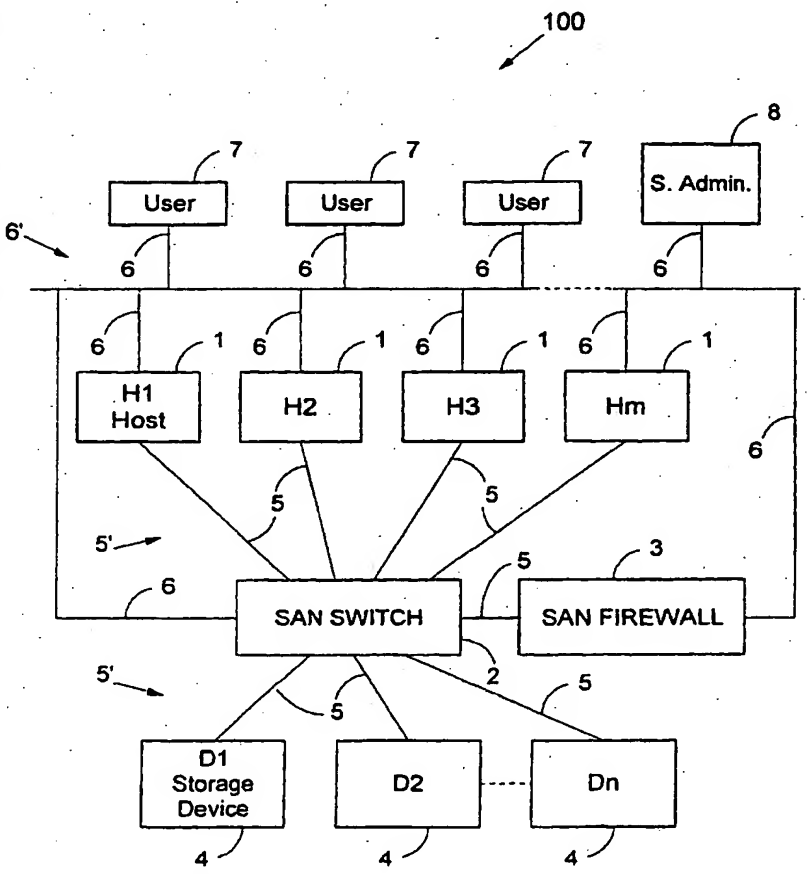
(74) Agent: LOWY, Avi; Glucksman-Lowy, P.O. Box 6202, 31061 Haifa (IL).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM),

[Continued on next page]

(54) Title: STORAGE AREA NETWORK (SAN) SECURITY



(57) Abstract: A method for the binary zoning of a Storage Area Network (SAN) for security is disclosed, for a SAN with physical devices consisting of a first array of hosts (1) and a second array of storage devices (4), and a SAN Switch (2, 2A) coupled intermediate the hosts and the storage devices. The SAN Switch routes I/O commands and accepts zoning commands. The method is based on starting operation of the SAN with mutually isolated physical devices and accepting zoning commands only after running security verification procedures requiring that hosts be authenticated and that storage devices be identified. Zoning is dynamically controlled from a workstation (8) operated by a System Administrator entering meta-zoning instructions, which are used to automatically program the zoning of the SAN Switch for legitimate physical devices. The method is implemented for security and booting of a SAN.

WO 02/071224 A1

European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

STORAGE AREA NETWORK (SAN) SECURITY

Technical Field

The present invention relates to the field of Storage Area Networks (SAN) in general and more particularly, to the security and booting of a SAN.

Background Art

Fig. 1 is a block diagram of a prior art Storage Area Network (SAN), which comprises an array of host computers 1, or hosts 1 (H1, H2, ..., Hm) coupled via a SAN Switch 2, to an array of storage devices 4 (D1, D2, ..., Dn). In Fig. 1 the number of hosts 1 and of storage devices 4, is limited but sufficient for illustrative purposes. The hosts 1, the SAN Switch 2 and the storage devices 4 are coupled by Fibre Channel (FC) links 5, or storage network links 5, in a storage network 5', forming a SAN Fabric. A Fabric is a Fibre Channel Network. Users network links 6, pertaining to a user network 6', connect users 7, a System Administrator 8, and the SAN Switch 2, to the hosts 1. The user network is an Ethernet, such as a LAN, a WAN, or the Internet.

It is noted that the SAN Switch 2 is also known in the art as Fiber Channel Network Switch, or Fiber Channel Switch or Network Channel Switch. Storage devices also referred to as storage subsystems, neither being necessarily of the same kind. The term storage device relates to all kinds of storage in use with digital data, such as disks, tapes, etc .

The SAN Switch 2, which is operated for routing I/O communications between the array of hosts 1 and the array of storage devices 4, is also utilized for zoning functions, in an attempt to provide al least some measure of security. The array of hosts 1 and the array of storage devices 4 are related to as the physical devices of the SAN.

A zone is defined a group of physical devices sharing permission for mutual communication. Practically, zones are formed between ports residing in the SAN Switch 2, and coupled to the physical devices. The smallest possible zone is a group of at least one port linked to a host 1, or host port, and of at least one port pertaining to a storage device 4, or device port, to which the SAN Switch 2 grants permission for mutual communication. The number of ports may be even or odd, but never less than two, to always couple between at least one host 1 and at least one storage device 4. Ports belonging to different zones cannot communicate with each other, and therefore, physical devices belonging to different zones, are isolated from each other. When a host 1 has more than one Host Bus Adaptor, HBA, then a zone is defined as a group sharing permission for mutual communication between HBAs and storage devices. Again, the minimum for one zone is one HBA and one storage device 4.

The SAN Switch 2 is coupled to both the storage network 5', by links 5, and to the users network 6', by links 6. One of those users 7 is defined as a System Administrator (SA) manning a SA workstation 8 privileged with access to the SAN Switch 2 via the users network 6'. By operating his workstation 8, the System Administrator may manually define zones of ports coupled to physical devices. Once defined, those zones are set and remain static.

What the SA actually defines, is the zoning of ports connected to hosts 1 and to storage devices 4, each port having an identity number. The mere connection of a port number does not vouch for the identity of the physical device that is intended to be, or is actually, connected to that port.

It is recognized that the conventional zoning exercised by the SAN Switch 2 presents security loopholes. Modern SAN systems consist of arrays with numerous hosts 1, away and remote from the SAN, easing the disguise of a fake host 1 as a genuine computer. Even though the SAN Switch 2 is coupled directly to a host 1, the former is not equipped with means able to block a rogue host from joining the storage network 5' in disguise, by adopting a fake identity and posing as a legal host 1. Actually, the SAN Switch 2 recognizes a host 1 only by the port number, without any provisions for the detection of a false identity hiding behind that port number.

Sometimes, the SA uses the WWN (World Wide Name) of a HBA (Host Bus Adaptor) to identify a host 1. Each host 1 has at least one HBA, and each HBA is identified by the 8 bytes of its unique WWN number. However, there is nothing to certify that a given HBA with a WWN is really running in a host 1 legally coupled to the SAN. With computer crime on the increase, it is plausible to expect trials to couple a fake host 1 to a SAN. In view of the foregoing, it is therefore maintained that the security of the SAN Fabric is in danger and includes loopholes.

The connection of a large numbers of physical devices inevitably results in a huge number of ports, all ports being manually zoned by the SA. Almost certainly, the manually performed zoning of dozens of ports will lead to coupling mistakes. This practice, prone to human errors, creates another type of security flaws since although the System Administrator zones groups of specific physical devices together, one single mistaken coupling may add an uncalled for physical device into a zone.

For example, a mistake like connecting a storage device 4 to a wrong port in a SAN Switch 2 may cause data corruption. In other words, a storage device 4, intended for connection to a specific port may be mistakenly, or perhaps intentionally, coupled to a port other than the intended specific port. It should be noted that the SAN Switch 2 does not

recognize a storage device 4 by identity, but only recognizes the physical ports, assuming that the intended storage device 4 is appropriately linked thereto. Again, a security problem may develop, especially if a connection is intentionally mistaken. These examples illustrate some typical security flaws of the zoning-function of the SAN Switch 2.

There is thus a need to provide security measures to SAN networks, and to prevent unauthorized access due to either human error or criminal intentions. Such unauthorized access usually occurs at ports, because of a mistakenly made connection or of the coupling of an illegal physical device.

Consideration should also be given to the fact that a SAN is not a static facility with a frozen configuration, since hosts 1 and storage devices 4 are frequently added or deleted. An addition usually indicates an intentional expansion of resources, while a deletion may point to an accidental failure. Since a SAN Fabric is subject to instant configuration change, there is a need for dynamic security monitoring capabilities. Most of all, it is recognized that a tool is absent which might permit the remote dynamic management of the security of a SAN, under automatic control of a computer program.

Presently, there is an acute need for the provision of both data storage and data transfer security. This need is especially emphasized in view of the growing intricacy of systems as well as to the escalation of criminal activity.

SUMMARY

It is an object of the present invention to provide a method for securing and for booting a SAN according to binary zoning for implementing authentication and identification in default zoning when physical devices are isolated and for zoning according to meta zoning instructions for zoning only those physical devices verified as legitimate.

There is provided a method for a Storage Area Network (SAN) security with booting, and with physical devices having a first array of hosts (1) and a second array of storage devices (4), a storage network (5') with network links (5), and a users network (6') with users network links (6). A SAN Switch (2, 2A) is coupled intermediate the first array and the second array and to each physical device via network links and to the users network via a users network link. The SAN Switch routes I/O commands to the physical devices and is configured for accepting zoning commands defining zones for communication between at least one host and at least one storage device. The method operates binary zoning for security with default zoning and work zoning permitting the creation of, respectively, at least one default zone and at least one work zone. The binary zoning always first resides in default zoning, and the default zoning, mutually isolates each one of the physical devices, and runs a

security procedure on each one of the physical devices for legitimacy verification, and in work zoning, zones only legitimate physical devices.

There is provided further a method for running, in default zoning of the security procedure and thereafter, creating, in work zoning, of at least one work zone comprising at least one legitimate host and at least one legitimate storage device. The method moreover provides running the security procedure that further comprises the steps of running an authentication procedure for presence and legitimacy verification of each one host out of the first array, and an identification procedure for presence and legitimacy verification of each one storage device out of the second array.

There is provided yet further a method for running continuously the security procedure for presence and legitimacy verification of the physical devices actually coupled in operation with the SAN, and rezoning in real time of the at least one work zone according to configuration changes associated with running the security procedure continuously.

There is provided yet further a method for securing a host with at least one HBA which is identified by a first WWN (World Wide Number), and a storage device comprises at least one LU (Logical Unit), and identified by a second WWN and by at least one LUN (Logical Unit Number). The security procedure authenticates each one host out of the first array independently of the first WWN, and identifies each one storage device out of the second array by the second WWN and by the at least one LUN.

There is provided additionally a method for a System Administration (SA) workstation coupled to the users network and to the SAN Switch. The SA workstation is configured for managing, securing and booting the SAN, and for entering meta-zoning instructions via the SA workstation. The meta-zoning instructions define programming commands for automatically deriving default zoning and work zoning, and programming automatically the SAN Switch, according to the meta-zoning instructions, into default zones and work zones.

There is provided further a method for controlling dynamically the binary zoning of the SAN Switch by entering meta-zoning instructions via the SA workstation. The method refers to the SAN having at least one HBA in each one host out of the first array, and the meta-zoning instructions carrying instructions for zoning, in a work zone, at least one HBA pertaining to a legitimate host with at least one legitimate storage device.

It is an object to provide a method with the SAN having at least one legitimate host out of the first array, with a plurality of HBAs. The meta-zoning instructions provide instructions for zoning in a work zone, each one out of the plurality of HBAs inside a legitimate host, with at least one legitimate storage device.

It is also an object to provide a method for burning-in the default zones in the SAN Switch, for automatically returning to and always start operation in default zoning, wherein the physical devices are mutually isolated. Furthermore, the SAN Switch comprises a plurality of ports, each port out of the plurality of ports having a port identity, and each one physical device is coupled to at least one port out of the plurality of ports. The security procedure is further characterized by comprising the step of verifying the legitimacy of each one of the physical devices independently of the port identity of the at least one port to which one physical device is coupled. In addition, the method deals with the SAN Switch comprising a plurality of ports, for coupling each one physical device to at least one port out of the plurality of ports, the method being further characterized by returning immediately the at least one port from which a physical device is decoupled, to a default zone. Moreover, there is provided a method where each one a port out of the plurality of ports of the SAN Switch always resides in a default zone when being coupled to a physical device.

It is another object yet to provide a method for Storage Area Network (SAN) booting. The SAN has physical devices with a first array of hosts (1) and a second array of storage devices (4). The SAN also has a storage network (5') with network links (5), a users network (6') with users network links (6), and a SAN Switch (2) coupled intermediate the first array and the second array and to each physical device via network links and to the users network via a users network link. The SAN Switch routes I/O commands to the physical devices and is configured for accepting zoning commands defining zones for communication between at least one host and at least one storage device. The method operates a binary zoning for booting, with default zoning and work zoning permitting the creation of, respectively, at least one default zone and at least one work zone. The binary zoning always first resides in default zoning for booting the first array of hosts in mutual isolation and starting the second array of storage devices, for verifying operation of the physical devices, and in the work mode zoning, having only operative physical devices.

It is another one more object to provide a method for configuring the storage network as a Fibre Channel network. The method comprises running the boot procedure and thereafter, creating, in work zoning, of at least one work zone comprising at least one operative host and at least one operative storage device. The method also comprises the steps of running continuously the booting procedure for presence and operation verification of the physical devices actually coupled in operation with the SAN, and rezoning in real time the at least one work zone according to configuration changes associated with presence and operation of the physical devices actually coupled to the SAN.

The method still further provides a System Administration (SA) workstation coupled to the users network and to the SAN Switch, for entering meta-zoning instructions via the SA workstation, the meta-zoning instructions defining default zoning and work zoning, and for programming automatically the SAN Switch into work zones for operative physical devices according to the meta-zoning instructions. The method comprises burning-in the default zones in the SAN Switch, for automatically returning to and always start operation in the default zoning, wherein the physical devices are mutually isolated. Another aspect of the method provided is that the SAN Switch comprises a plurality of ports, for coupling each one physical device to at least one port out of the plurality of ports, the method being further characterized by returning immediately the at least one port from which a physical device is decoupled, to the default zone. A port out of the plurality of ports of the SAN Switch always resides in a default zone when being coupled to a physical device.

Still further, the method provides for a SAN Firewall packaged with the SAN Switch to form a single unit, and for the SAN Firewall and the SAN Switch to be functionally integrated to form a single unit package. The SAN Firewall functions operate on a host selected from the first array, or on a remote host coupled to the SAN Switch, or on a remote host coupled to the SAN Switch via a network link coupled to a global communication network.

It is yet another object of the invention to provide a system for operating SAN security and booting, with physical devices comprising a first array of hosts (1) and a second array of storage devices (4), a storage network (5') with storage network links (5), and a users network (6') with users network links (6). There is also a SAN Switch (2) coupled intermediate the first array and the second array and to each physical device via network links, and coupled to the users network via a users network link, the SAN Switch routing I/O commands to the physical devices. SAN Switch (2) is configured for accepting zoning commands defining zones for communication between at least one host and at least one storage device. The SAN Switch comprises a plurality of ports for coupling each one of the physical devices to at least one port out of the plurality of ports by at least one network link (5). The system with the SAN Firewall (3) is coupled by a storage network link to a SAN-Firewall-port (sf) accommodated in the SAN Switch and coupled by a user network link to the users network, the SAN Firewall being configured to automatically program the SAN Switch into zones, with each zone residing in either one of a binary zoning. The binary zoning comprises, in default zoning, at least one default zone counting only two ports, with a first SAN-Firewall-port coupled to the SAN Firewall and connected to a second device-port (h, d) coupled to and isolating a physical device, the SAN Firewall operating at least one security verification procedure on the isolated physical device. In work zoning, there is at least one work zone

coupling at least three ports, with a single SAN-Firewall-port (sf), and at least two ports coupling only security verified physical devices counting at least one host port (h), and at least one storage device port (d).

There is provided, according to the system for SAN booting, physical devices with a first array of hosts (1) and a second array of storage devices (4), a storage network (5') with storage network links (5), and a users network (6') with users network links (6). There is also a SAN Switch (2) coupled intermediate the first array and the second array and to each physical device via network links, and coupled to the users network via a users network link. The SAN Switch routes I/O commands to the physical devices and is configured for accepting zoning commands defining zones for communication between at least one host and at least one storage device. The SAN Switch comprises a plurality of ports for coupling each one of the physical devices to at least one port out of the plurality of ports by at least one network link (5). The SAN Switch is configured for default zoning wherein each port out of the plurality of ports for coupling to a physical device is a mutually isolated default zone and the default zoning is burnt-in in the SAN Switch to always start operation in default zoning, whereby the physical device are mutually isolated. In addition, there is verified the operation of at least one host of the first array, and operatively zoning the at least one operative host with at least one storage device.

One object is to provide a Security Computer Program (SCP) operating with a SAN for security and booting. The SAN has physical devices comprising a first array of hosts (1), a second array of storage devices (4), and a third array of user workstations (7) comprising a System Administrator (SA) workstation (8). Each one host of the first array comprises at least one Host Bus Adaptor (HBA), and a SAN Switch (2, 2A) intermediate the first array and the second array, for routing I/O commands to the physical devices and for accepting zoning commands, the SAN Switch comprising a plurality of ports. There is also a storage network (5') with network links (5) coupling the SAN Switch to each one of the physical devices and to at least one port out of the plurality of ports by at least one network link (5). The SAN Switch routes I/O commands to the physical devices and is configured for accepting zoning commands defining zones for communication between at least one host and at least one storage device. Provided additionally is a users network (6') with network links (6) coupled to the third array, to the SAN Firewall and to the SAN Switch. The SCP has at least one SAN Agent and a Firewall Software operating in mutual association, with an at least one SAN Agent operating in each one host out of the first array, and the Firewall Software operating in the SAN Firewall. The Firewall Software has a binary zoning program with default zoning and work zoning, for zoning in response to commands derived from meta zoning instructions,

comprising defaults zones and work zones. These have a default zone operating on two ports only, the first port being a SAN Firewall port (sf) to which the SAN Firewall is coupled and the second port being either one of a host port (h) and a storage device port (d) to which one physical device is coupled. Each default zone mutually isolating the physical device, to perform at least one security and booting procedure in isolation. A work zone consists of only physical devices verified by the verification procedure intended for coupling at least one host and at least one storage device in associative operation, the default zone comprising at least one host port, one storage device port and the SAN Firewall port.

Another object of the Security Computer Program, in the SAN Agent, is to provide an identity key being sent in periodic repetition to the Firewall Software, and in the Firewall Software, a host authentication procedure of the verification procedure for operation with a host identity key received from a SAN Agent. A storage device identification procedure is included in the verification procedure whereby the Firewall Software accesses each one storage device of the second array to check identity parameters with a World Wide Name (WWN) and an at least one Logic Unit Number (LUN).

The Security Computer Program provides running continuously of the security procedure for presence and legitimacy verification of the physical devices actually coupled in operation with the SAN, and for rezoning in real time the at least one work zone according to configuration changes associated with running the security procedure continuously.

There is provided a Security Computer Program with, in default zoning, an HBA is identified by a first WWN (World Wide Number), a storage device comprises at least one LU (Logical Unit), and identified by a second WWN and by at least one LUN (Logical Unit Number). There is also a list of presence operated and updated by the Firewall Software to record instant configuration of the physical devices coupled to the SAN with identifiers for each host of the first array. This includes a first WWN of an at least one HBA, and for each storage device of the second array, a second WWN and at least one LUN, and port identity coupled to physical devices at the SAN Switch. The security procedure has, in work zoning, a status map recording the instant configuration of legitimate physical devices coupled to the SAN with the identifiers. Therein, each one host out of the first array is authenticated independently of the first WWN and of the at least one HBA name, and each one storage device out of the second array is identified by the second WWN and by the at least one LUN.

It is yet another object to provide a Security Computer Program operating with a SAN for booting, the SAN having physical devices with a first array of hosts (1) and a second array of storage devices (4), a storage network (5') with network links (5), and a users network (6') with users network links (6). The SCP has a SAN Switch (2) coupled intermediate the first

array and the second array and to each physical device via network links and to the users network via a users network link. The SAN Switch routes I/O commands to the physical devices and is configured for accepting zoning commands defining zones for communication between at least one host and at least one storage device. The SCP operates a binary zoning program for booting, with default zoning and work zoning permitting the creation of, respectively, at least one default zone and at least one work zone, the binary zoning program always first residing in default zoning. In default zoning, booting the first array of hosts in mutual isolation and starting the second array of storage devices, for verifying operation of the physical devices, and in the work zoning, having only operative physical devices.

There is provided additionally, a listing procedure for listing the physical devices coupled to the SAN Switch, a status map procedure for building and maintaining the status map recording the legitimate physical devices coupled to the SAN Switch, and a work zone procedure for commanding automatic zoning of legitimate physical devices recorded in the status map.

BRIEF DESCRIPTION OF THE DRAWINGS

In order to understand the invention and to see how it may be carried out in practice, preferred embodiment will now be described, by way of non-limiting examples only, with reference to the accompanying drawings, in which:

Fig. 1 is a block diagram of a prior art SAN,

Fig. 2 is a block diagram of a SAN equipped with security monitoring,

Fig. 3 shows an example of default zoning of the SAN Switch of Fig. 2,

Fig. 4 depicts an example of a work zoning for the configuration of Fig. 3,

Fig. 5 is an example of default zoning for more than one HBA per host,

Fig. 6 illustrates an example of work zoning for the configuration of Fig. 5,

Fig. 7 presents a flowchart of the boot procedure of a host,

Fig. 8 is a flowchart of the procedure for physical device discovery and recognition,

Fig 9 depicts the main hardware structural blocks of the SAN Firewall 3,

Fig. 10 illustrates details of the elements of the Fibre Channel Interface Board,

Fig. 11 shows the principal software modules of the SAN Firewall 3,

Fig. 12 is another embodiment of the SAN security shown in Fig. 2,

Fig. 13 presents a further embodiment of the SAN security depicted in Fig. 2, and

Fig. 14 exemplifies still another embodiment of the SAN security of Fig. 2.

DESCRIPTION OF PREFERRED EMBODIMENTS

The necessity to provide means to authenticate hosts 1 and to ascertain the identity of storage devices 4 was explained above. A solution to the lack of security in a SAN may be provided by enforcing the following steps. First, requiring the authentication of each host 1; and second, in parallel, requesting identification of each storage device 4. Before permitting coupling between physical devices on the SAN network, these physical devices should be subjected to verification procedures, known to the art, available and reliable, that employ only limited processing resources. A third prerequisite is the elimination of manual port zoning commands, which must be replaced by meta-zoning instructions containing decisions taken by the System Administrator for further automatic zoning of the SAN Switch 2. This means that the SA makes decisions and that the actual zoning chores are performed automatically by software, hardware or a combination thereof.

One may consider a SA entering meta-zoning instructions at his workstation 8, which means, deciding what host, or hosts 1, will be zoned to operate together with one or more storage device 4. Then, according to the present invention, each host 1 in turn will be authenticated, instead of the one or many HBAs the host houses, and in place of the ports of the SAN Switch 2.

In other words, the HBA(s) of a host 1 that is positively authenticated as legitimate, become(s) automatically legitimate as well. Storage devices 4, after being affirmatively identified, also become legitimate. The identity of the ports now becomes irrelevant for security purposes. Incidentally, a storage device 4 is identified by the 8 bytes of is WWN and by the 8 bytes of its Logical Unit Number (LUN).

In the context of this disclosure, the term "legitimate" is considered as meaning: "screened for security purposes and accepted as a genuine and authentic physical device."

In operation, the configuration of a SAN is not static: the SA may decide to add resources, or on the contrary, physical devices sometimes fail or are removed for maintenance purposes. The solution proposed by the invention will regard any physical device added to the SAN network as suspect and unaccepted until authenticated or properly identified. Moreover, the disconnection of a physical device causes the immediate removal of the port to which it was connected from the zone(s) in which it was operative.

Fig. 2 shows a first embodiment 100. The same numerals refer to the same elements in the various Figures. The SAN supports an array of m hosts 1 and of n storage devices 4, with users 7 and 8 coupled to the user network 6'. The SAN Switch 2 is coupled to a SAN Firewall 3 that is also linked to a SA workstation 8, acting as both a System Administration workstation and a Security Administration workstation. Possibly, a separate Security

Administration and a separate System Administration workstation 8 may be coupled to the SAN instead of the single SA workstation as depicted in Fig. 2. It is noted that both the SAN Switch 2 and the SAN Firewall 3 are equipped with processing means supported by memory, and configured to run computer programs stored in magnetic memory.

The SAN Firewall 3 is coupled to the SAN Switch 2 by a storage network link 5 and to the user network 6' by a user network link 6. Although obvious, it is important to note that the SAN Firewall 3 may gain access to the SAN Switch 2 via either a storage network link 5 or a user network link 6. This feature allows communication between the HBA(s) of any host(s) 1 and the SAN Firewall 3.

The SA workstation 8, coupled to the user network 6', is privileged with direct access to the SAN Firewall 3. Accordingly, the SA Administrator may operate the SA workstation 8 to send meta-zoning instructions to the SAN Firewall 3, which in turn, will take care of the automatic programming of the SAN Switch 2 into zones, according to those meta-zoning instructions.

For monitoring of security, the SAN Switch 2 is programmed to operate in binary zoning: first in default zoning and next, in a work zoning. The default zoning creates default zones, which are "dead end" zones, leading only to a SAN Firewall port sf coupled to the SAN Firewall 3, and to a port connected to a physical device, either a host port hp or a storage device port dp. Each default zone acts as a secluded check-zone wherein an authentication or identification procedure is operated on the physical devices via the SAN Firewall port sf, before granting permission for inter-connection and zoning with other physical devices of the SAN. In other words, a default zone may be regarded not as a zone but as a singular condition of zero zoning, or no zoning at all.

To keep the description simple, it is first assumed that each host 1 has only one Host Bus Adaptor, or HBA.

Inside the SAN Switch 2, each default zone is limited to but one single connection between one specific physical device of the SAN and the SAN Firewall 3. The first end of the connection link is coupled to either a host 1 or a storage device 4, and the second end of the same link is coupled to the SAN Firewall 3. In other words, each physical device remains isolated and captive within one default zone while in default zoning. Furthermore, the number of default zones equals the sum of the physical devices coupled to the Switch 2. Assuming an array of hosts 1 designated as (H1, H2, ..., Hm) where each host has only one HBA, and an array of storage devices 4 labeled as (D1, D2,..., Dn), there are then m + n separate default zones, all coupled to the SAN Firewall 3. When any of the hosts 1 has more than a single

HBA, then the number of default zones is the sum of the total number of HBAs in all the hosts and of the number of storage devices 4.

It is appreciated that although reference is made to a single SAN Switch 2, that switch may be built out of a plurality of switches coupled in one of the various known circuit connection manners to form one larger switch, which is regarded to perform and respond as if being configured as one single SAN Switch 2. It is also noted that the coupling of switches is well known to the art and therefore, needs not to be described.

Reference is now made to Fig. 3 to illustrate a simplified example of default zoning connections in the SAN Switch 2. Only a portion of the SAN is shown, with an array of three hosts 1, H1, H2, and H3, connected to host ports, respectively h1, h2, and h3. In this example, there is only one HBA per host.

In the same manner, three storage devices 4, D1, D2, and D3, are connected to an array of storage device ports, respectively d1, d2, and d3. In addition, one SAN Firewall port, designated as sf, is linked to the SAN Firewall 3. In Fig. 3, each dotted line designated as DZ, leading from the port sf to the port of one physical device, represents one single default zone, clearly illustrating that each default zone is isolated from any other default zone. This default zoning is burnt-in into the SAN Switch 2 and will always prevail on start-up. The default zoning is thus inherently reset on each shut down, always initiating a SAN start in default zoning. Furthermore, on disconnection of a physical device from a port of the SAN Switch 2, that port will automatically be isolated in a default zone. Therefore, upon coupling to a port of the SAN Switch 2, a physical device will always meet a default zone.

The security procedures described below, are all performed while the SAN Switch 2 resides in default zoning, to ascertain the authenticity of each host 1 and the identity of each storage device 4 before allowing the coupling of any communication between these physical devices 1 and 4. Next, in work zoning, where the physical devices are coupled in mutual operative association, work zones are defined only after successful completion of the security checks and procedures. These work zones are derived from meta-zoning instructions defined at the SA workstation 8 and communicated via the user network 6' to the SAN Firewall 3, the latter generating commands for the automatic programming of the SAN Switch 2 into separate and distinct work zones.

For the sake of illustration, it is assumed that an SA manages a SAN with three hosts 1, namely H1, H2, H3, and with three storage devices, denominated D1, D2, D3, as depicted in Fig. 3. It is further assumed that the SA meta-zones the access of the selected hosts 1 with the following specific storage device 4, in work zones defined in Fig. 3: hosts H1 and H2 with storage device D3, host H2 and storage device 2, again hosts H1 and H2 but now with storage

devices D1 and D2, and finally host H3 also with storage devices D1 and D2. These access permissions are the meta-zoning instructions, defined by the SA via his SA workstation 8, also related to as a Permission Table, shown below as Table 1.

WORK ZONE No.	HOST	STORAGE DEVICE
1	H1, H2	D3
2	H2	D2
3	H1, H2	D1, D2
4	H3	D1, D2

Table 1

The meta-zoning instructions presented in Table 1 are flexible and easily changeable, allowing for addition, or deletion, independently of physical devices and of work zones. In Table 1, the empty rows indicate that more physical devices may be added to the SAN, all to be managed in the same way. Evidently, during the operation of a SAN, hosts 1 and storage devices 4 may be retrieved from the network, by either deleting their access permission, or by physical removal, for maintenance for example, or as result of a crash.

The meta-zoning instructions entered by the SA at the SA workstation 8, designate hosts 1, or the HBAs of these hosts 1, for coupling with storage devices 4. It is understood that the task of the SA is supported by details pertaining to the physical devices, such as the WWN of HBAs, the WWNs and LUNs of storage devices, identity parameters and other necessary details being automatically presented on screen and added to the meta-zoning instruction at the SA workstation. Such information is possibly entered as a permission table.

A SAN Security Computer Program, or SCP for short, is operative on the SAN to perform the security clearance of the physical devices, to receive meta-zoning instructions from the SA workstation 8, to automatically program the SAN Switch 2 accordingly into working zones, and to dynamically control the security of the instant configuration of the SAN in real time.

Fig. 4 depicts an example of the work zones in the SAN Switch 2, showing the four automatically programmed work zones, as derived from the meta-zoning instructions of Table 1, for the configuration of physical devices 1 and 4, shown in Fig. 3. It is noted that a work zone always consists of at least three ports, namely the SAN Firewall port sf and at least one port of each a host 1 and a storage device 4. The first work zone Z1 is formed by the ports h1,

h2 and d3, a second work zone Z2 consists of the ports h2 and d2, a third work zone Z3 involves the ports h1, h2, d1 and d2, and last, a fourth work zone Z4 includes ports h3, d1 and d2. The automatic derivation of work zones from the meta zoning instructions is achieved by help of a computer program currently provided by the manufacturer of the SAN Switch 2, such as for example, Brocade Communications Systems, Inc., of 1745 Technology Drive, San Jose, CA 95110, USA, manufacturer of the Model called Silkworm 2800.

It is noted that the work zones are created solely on the basis of the meta-zoning instructions that specify only hosts 1 and storage devices 4, as transmitted to the SAN Firewall 3.

The SCP consists essentially of two different portions, each portion running possibly in a different location but remaining in communication for interactive operation. A portion of the real-time SCP runs in the SAN Firewall 3 to automatically program the SAN Switch 2, in contrast with the manual input of the port-to-port connections for zoning, as by the prior art. Therefore, since the physical devices are coupled into zones according to their authenticity and identity, and not according to their port number at the SAN Switch 2, the possibility of a manual connection error is eliminated: manual connection are not needed anymore.

The first portion of the SCP, or Firewall Software, runs in the SAN Firewall 3, sometimes referred to as the Firewall Configuration Software. The second portion of the SCP operates in each one of the hosts 1, and is related to as the Firewall Agent, or Firewall Service. Each one of the hosts 1 controls the operation of its own Firewall Agent.

When in the default zone, before access is permitted to work zoning, each single one of the various physical devices of the SAN is interrogated for verification, but the security procedure is different for the hosts 1 and for the storage devices 4. After verification, described below, only the positively identified physical devices are approved and mapped in a Status Map managed by the SAN Firewall 3. The Status Map lists identified and authorized physical devices, their identity, the HBAs and the port numbers of the SAN Switch 2. Physical devices 1 and 4 that are not security approved by the SCP are kept isolated and remain in default-zoning mode.

On start-up, the SAN Switch 2 always starts in default zoning, as explained above. The presence and identity details of each separate physical device coupled to a port of the SAN Switch 2 is collected by the SAN Firewall 3 via the SAN Firewall port sf. Such details include, among others, the WWN of each HBA, the WWN and the LUN of each storage device 4 as well as the related port number identity.

Each booted host 1 coupled to the SAN is submitted to a security procedure, such as an encrypted authentication procedure. The login is accompanied by, for example, an identity

key, inserted a priory by the SA, being sent via an HBA, to the SAN Firewall 3. In the beginning, before authentication, the host 1 is listed, as being a physical device coupled to the SAN, but is not yet approved. It is then that an appropriately selected available authentication computer program is operated by the Firewall Software to authenticate that host 1. Evidently, the identity key presented for verification was previously inserted in that host 1 by the SA, to operate in association with the authentication computer program run by the SAN Firewall 3. This same procedure is repeated for all the hosts 1 coupled to the SAN, listing all the HBAs, when there is more than one HBA per host.

When the identification key matches the requirements of the Firewall Software encrypted authentication procedure, then, and only then, is the host 1 authenticated and listed in the Status Map as valid for work zoning purposes. At the same time, the WWN of each HBA residing in that host 1 and the associated port number is listed and is added to the Status Map. On the contrary, if the host 1 is for example a rogue plugged into a port of the SAN Switch 2, the identity key will not match, or be missing. That rogue host 1 is then considered as negative, regarded as illegal, kept safely isolated in a default zone and evidently not listed in the Status Map.

Authentication computer programs are known in the art, and for the purpose of host identification, any suitable authentication program fitting the task may be selected.

The identification procedure for a storage device 4 coupled to the SAN is initiated by a polling procedure run by the Firewall Software. Polling queries pass from the SAN Firewall 3 through the default zone of the SAN Switch 2, via the storage link 5 to the interrogated storage device 4. The Firewall Software questions each storage device 4 in turn for identity, by requesting both its WWN and its Logical Unit Number, or LUN. When both the requested WWN and the LUN match those fitting and corresponding to the storage devices 4 according to the meta-zoning instructions previously entered by the SA, then that WWN, together with the LUN of the storage device 4 and the port number are listed in the Status Map along with the legal and authorized storage devices. Else, the storage device 4 is regarded as illegal, kept secluded in a default zone of the SAN Switch 2, and does not appear in the Status Map.

As a consequence of the security procedures, the Status Map now contains solely authorized hosts 1, their respective HBAs, authorized storage devices 4, and the associated port numbers.

It was already mentioned that to enhance security, the work zoning configuration of the SAN Switch 2 is never saved, but built anew from scratch, after every power-up of the SAN, thus starting from default zoning. Upon uncoupling of an authorized physical device from a port, that port automatically returns to default zoning so that the coupling of a physical device

to an available port always meets a default zone. An unauthorized host, when uncoupled from a port, always leaves a default zone, but will be deleted from the list of physical devices coupled to the SAN..

In practice, a host may comprise more than one HBA and each HBA terminates as a port, or host port, in the SAN Switch 2. The result is that the number of coupled ports in a SAN Switch 2 now actually equals at least to the sum of the number of HBAs of all the hosts 1, plus the number of all the storage devices 4, plus one SAN Firewall port. For the sake of exactitude, in practice, a second SAN Firewall 3 is used for redundancy purposes, thereby increasing the number of ports. This redundant SAN Firewall 3 is not shown in the Figs., and is not referred to below, to keep the description simple.

A simplified illustration with more than one HBA per host 1 is presented in Fig. 5. The array of hosts 1 is limited to a first and to a second host, respectively H1 and H2, where the first host features two HBAs, namely HBA1,1 and HBA1,2, each having an access port at the SAN Switch 2, respectively h1,1 and h1,2 . The second host H2 has only one HBA, designated as HBA2,1, corresponding to a port indicated as h2, 1.

A work zoning example of the configuration of ports shown in Fig. 5 is depicted in Fig. 6. For zoning purposes, it is possible to simply envision each HBA as a host 1 with a single HBA, so that the various HBAs form an enlarged array of hosts 1. Such visualization refers back to and reinstates the description related to Fig. 3. As an illustration, Fig. 6 depicts the identical number of zones with the identical number of ports as in Fig. 4.

Host Boot

With reference to Fig. 7, the operation of the SAN Security Program, SCP, is now described. When a host 1 is booted, as in step 50, in mutual isolation from the other hosts 1, the Firewall Agent, running in that host 1, is loaded, by step 51. The Firewall Agent searches for the SAN Firewall 3 in step 52, and reaches a bifurcation in step 53. If the SAN Firewall 3 is absent, then step 54 allows for boot-up without communication links to SAN storage devices 4. Step 55 is a temporary end of procedure, before returning for another try to find the SAN Firewall 3.

However, if step 53 finds the SAN Firewall 3, then, as in step 56, the host 1 sends the identity key, for unique encrypted identification, to the Firewall Software running in the SAN Firewall 3. In turn, step 57 awaits the authentication decision: a negative outcome ends the procedure and keeps the host 1 in question isolated, with the Firewall 3 as a barrier, as by step 58. . Possibly, but not shown in Fig. 7, other trial follow. Conversely, a positive identification results in the authentication of the host 1, as in step 59, and the listing of the host as well as of

the WWN(s), the port numbers of the one or more HBA(s), into the Status Map. That host 1 is now recognized and tagged as legitimate for work zoning purposes, and the at least one HBA of the host is thus security-wise accepted to operate in association with one or more authorized storage device(s) 4 according to the specific work zones programmed by the SAN Firewall 3 into the SAN Switch 2. Step 60 ends the security procedure for a host 1.

The identification of storage devices 4 is considered in the context of the SAN working environment as being dynamic, where physical devices are sometimes added or removed. For instance, storage capacity may be increased or reduced by the SA, or by malfunction when a storage device crashes. The same is valid for the computing power, relating to the hosts 1.

In Fig. 8, the identification procedure of a storage device 4 is described, as a part of the procedure for the handling of newly discovered physical devices.

On start-up of the SAN, step 600 conducts a search in default zoning, since the SAN Switch 2 always starts in default zoning, on all the ports coupled to physical devices. The search is initiated by the SAN Firewall 3, on the instant configuration of physical devices coupled to the SAN. A deleted physical device becomes automatically non-accessible to the search, but a new physical device must be detected, verified, and zoned, to become effective. New hosts 1 announce themselves sequentially via their HBA(s) to the SAN Firewall 3, while that same SAN Firewall sequentially initiates searches for new storage devices 4. Hence, if a new physical device is detected by step 601, the search procedure continues, but else, command returns to step 600, for another search, in constant repetition, for continuous real time update. Whenever a new physical device is found, in step 601, it is necessary to distinguish between a host 1 and a storage device 4.

For a storage device 4, in step 603, the WWN and the LUN are checked for identity, to match with a list of such devices entered as a permission table at the time of meta zoning. An invalid storage device 4 is isolated in step 604, while for a legitimate storage device 4, the procedure passes to step 605. There, it is checked if the storage device 4 is assigned by the SA in the meta-zoning instructions. If not assigned, then control flows to step 606, to display this fact on the SA workstation 8, and for return to step 600 for a further search. When the storage device 4 is detected by step 605 as being a member of a work zone, then the WWN, the LUN, and the port number thereof are added to the Status Map, and the storage device is authorized as a legal physical device of the SAN, as by step 607. Finally, another search starts after control is returned to step 600.

Step 602 responds to the detection of the announcement of a new host 1 by calling for an authentication certification test in step 608. The verification test is possibly based on any selected and available identity authentication method, with encryption techniques, and/or

public and private keys. An unauthorized host 1 is routed to step 609 and kept isolated. If the host 1 is authenticated, then step 610 checks if that host is listed in the meta zoning instructions. If so, then the next step 611 adds the one or more WWN(s) of the HBA(s) and the related port number(s) in the Status Map, and proceeds to step 600 for a further search loop.

SAN Firewall Structure

The main structural blocks of the SAN Firewall 3 are now presented as an example only, with reference to Fig. 9. A standard Pentium based Single Board Computer 70 (SBC 70) is connected to a Fibre Channel Interface Board 71 (FC-IB 71) through a PCI bus 72. The SBC 70 runs a Windows NT (Win NT) operating system featuring a built-in web-server for communication with the SA workstation 8 from where the security control is operated. The Win NT is necessary to allow the SA to access the FC-IB 71 from the SA workstation 8 linked to the users network, shown as an Ethernet link 6 in Fig. 9. Therefore, the SBC 70 also features an Ethernet port, not shown in Fig. 9 for the sake of simplicity, used to connect the SAN Firewall 3 to the user network by the Ethernet link 6. From the SA workstation 8 it is thus possible to access the SAN Switch 2 to program the zoning.

Details of the connections and of the processor of the Fibre Channel Interface Board 71 (FC IB 71) are not shown in Fig. 9. However, the FC-IB 71 operates under the control of an Ixworks real-time operating system (Ixworks RTOS) and is coupled by at least one Fiber Channel link 5 to the SAN Switch 2 shown in Fig. 1. Two FC links 5, for redundancy, are shown in Fig. 9.

Fig. 10 depicts in more details the elements of the Fibre Channel Interface Board 71, or FC-IB 71, shown in Fig. 9 as a building block of the SAN Firewall 3. An i960 RN processor 80 operates the Ixworks real time operating system of the SAN Firewall 3. The i960 RN processor 80 is coupled by a primary 64-bit bus PCI 81 to the SBC 70 seen in Fig. 9, and by a secondary 64-bit bus PCI 82 to a couple of Fibre Channel chips 83. There are two Fibre Channel chips 83 for redundancy purposes, although reference will be made to a single Fibre Channel chip 83. In addition, the i960 RN processor 80 is also linked by a SDRAM Interface 84 to a SDRAM DIMM memory 85 and by a Flash Bus Interface 86 to a non-volatile Flash memory 87. The Flash memory 87 contains the configuration and software of the SAN Firewall 3.

The FC chip 83 is a Qlogic chip that is connected to the SAN Switch 2 by a Fibre Channel Interface 88. Other elements connected to the FC chip 83 comprise an Optional Serial EEPROM 89 and a SRAM 90.

The primary PCI bus 81 is used for information exchange with the NT Operating System running on the SBC 70, shown in Fig. 2, to allow communication with the SA workstation 8. The secondary PCI bus 82 is coupled to the FC chips 83 for communication with the SAN Switch 2. More components are attached to the FC-IB 71 but are not described since they are standard and do not add to the explanations.

Referring now to Fig. 11, the principal software modules of the SAN Firewall 3 are depicted. The programs referred to as Pentium software programs are run by the Win NT on the Single Board Computer 70 (SBC 70) while those denominated as 960 programs are run by the i960 RN processor 80 on the FC-IB 71.

The software computer programs running on the Pentium comprises, amongst others, the Windows NT operating system 91 (Windows NT 91), with a standard TCP/IP stack 92, a web server 93, and an I2O device driver module 94. The I2O module 94 executes the data communication tasks between the Windows NT 91 and the Ixworks Real Time Operating System 95 (Ixworks RTOS 95) and retrieves the HTML pages used by the SA workstation 8 for configuration control and for zoning.

The 960 programs comprise the Ixworks Real Time Operating System 95 (IX RTOS 95) including a built-in I2O Support Module (not shown in Fig. 11). The I2O Support Module communicates with the I2O driver 94 of the Windows NT operating system 91. The IX RTOS 95 also runs the following software modules: an FC driver 97, a Disk/HBA driver 98, a Setup 99, and an HTML builder 101.

The FC driver module 97, programmed according to the Qlogic HBA firmware specifications, handles the FC software interface for communication of the SAN Firewall 3 with the SAN Switch 2. In other words, the FC driver module 97 enables FC communication between to the SAN Firewall 3 and the SAN Switch 2.

The HTML pages are generated by the HTML-builder 101 module for communication with the SA workstation 8.

Furthermore, the disk/HBA module is in charge of communications between the SAN Firewall 3 and the storage devices 4 as well as with each HBA in the hosts 1.

The Setup module 99 manages the Status Map and the permissions of access of the hosts 1 to the storage devices 4.

Additional Embodiments

Additional embodiments of the security and booting procedure are shown in Figs. 12 to 14.

In embodiment 200, in Fig. 12, the SAN Firewall 3 is integrated with the SAN Switch 2 to form a new SAN Switch 2A. For the sake of simplicity, the array of users 7 and the SA workstation 8 are not shown in Fig. 12. The integration configurations may span possibly only from the mere packaging of both the SAN Switch 2 and the SAN Firewall 3 into the same housing, up to the hardware and software integration of both, with many intermediate degrees of integration in-between. The new SAN Switch 2A operates and functions as each one of both the SAN Switch 2 and of the SAN Firewall 3 which it replaces. The linking to the network, is almost the same as with embodiment 100: the connection linking both former San Switch 2 and SAN Firewall 3 is now internal to the SAN Switch 2A. Two users network links 6, or only a single users network links 6 as shown in Fig. 12, are/is coupled to the SAN Switch 2A according to the level of integration of this last one. The new embodiment 200 is transparent to the SA.

A further embodiment 300 is illustrated in Fig. 13, where the functions of the SAN Firewall 3 are implemented as a software computer program SFW 300, not shown in Fig. 13, running on a chosen host 1A. For the sake of simplicity, the array of users 7 and the SA workstation 8 are not shown in Fig. 13. The SAN Switch 2 of the embodiment 100 is retained, in coupling over a users network link 6 with the SA workstation 8, to operate as with embodiment 100. For the sake of redundancy, a second computer program SFW 300, (not shown in Fig. 13) is installed on any other host 1. Embodiment 300 is transparent to the SA and operates together with the SCP's Firewall Agent running in the hosts 1 as well as in the chosen host 1A.

Still another embodiment 400 is depicted in Fig. 14 where the SCP's Firewall Software functions of the SAN Firewall 3 are implemented as a software computer program SFW 400, not shown in Fig. 14, installed in a remote host 1R. The host 1R is coupled to the array of hosts 1 by a user network link 6 via another network, such as any global communication network 80 or the Internet for example. The zoning commands reach the SAN Switch 2 over the storage links 5, as for the embodiment 400, and/or by a users network link 6 also coupled to the SAN Switch 2.

In contrast with the embodiments 200 and 300, the remote host 1R resides outside the SAN. The software computer program SFM 400 is possibly the same or similar to the SFM 300 used in embodiment 300, but may require adaptations related to network communication requirements.

The embodiments 100 to 400 emphasize the many possibilities of implementation of the security and booting of a SAN as a combination of hardware and software running on processors of various kinds and in various locations. Furthermore, the security and/or booting

is also easily implemented as dedicate hardware, or firmware, or software for operation on various processors or hosts 1. However, the SCP always retains two separate portions, namely the Firewall Agent and the Firewall Software.

SAN Booting

It is appreciated that the binary zoning method described above provides advantageous applications beyond security applications. For example, it is well known that on boot-up, each host 1 signals its active presence by emitting a notification message in the form of a communication on the storage network. Consequently, all the hosts on the network begin a physical device presence updating procedure, causing perturbations to the boot process due to the registration of the newly booted-up hosts with all the other hosts. This is why the prior art current practice in force is to boot each host separately by appropriate labor-intensive manual. Besides being tedious and time consuming, this process is prone to mistakes and connection errors. Therefore, the binary zoning provided by the security procedures of the SCP, whereby all the hosts 1 are initially isolated, automatizes the booting of SAN networks and is especially appreciated, and not only in the case large SAN installations with a multiplicity of hosts. Furthermore, the same advantage is beneficial when a host 1 is coupled to an operating SAN and booted up: since that host 1 encounters first a "dead-end" or default zone, and once operative, is coupled to a work zone, no perturbations are propagated.

Evidently, the SAN booting method is inherent to the SAN security method and is actually a SAN security and booting method. On boot-up, as for example by Fig. 2, each host 1 is isolated by the SAN Switch 2 in a default zone, as explained before. When indication is received that a host 1 is operative, that host is coupled to storage devices 4 in a work zone, as by the meta zoning instructions entered at the SA workstation 8. A booting implementation does not require any security procedure but only checks the operative status of the hosts 1. Here too, the SAN Switch 2 is burnt-in to always reside in the default zoning on start-up. A port from which a host 1 is uncoupled also immediately returns to a default zone. In parallel, when coupled to a SAN Switch port, a host 1 will always meet a default zone.

The booting of a SAN does not necessarily require a SAN Firewall 3. It is sufficient to keep the hosts 1 in isolation on boot-up, and after operation is detected, either by the SA or by any set-up added to the SAN Switch 2, to have the SA manually couple the physical devices in zones. To this end, it is sufficient to burn-in default zones, each default zone isolating a single port of the SAN Switch 2, since there is no SAN Firewall in this implementation. On boot-up, each host 1 meets a default zone. After detection that the host 1 isolated at a specific

port is operative, that port is zoned. Although less automatic, this scheme is easily implemented.

It is possible to explain the binary zoning security method implemented by the SCP as operating with a SAN Switch residing in either the closed ("OFF") state representing default zoning, or in the operative ("ON") state, which is the work zoning. The verification procedures applied to the physical devices when the switch is "OFF", and zoning is performed, after verification and legitimation of the physical devices in the "ON" state. This binary approach permits to implement SAN verification methods in a wide spectrum of combinations of hardware, software, and firmware.

It will be appreciated by persons skilled in the art, that the present invention is not limited to what has been particularly shown and described hereinabove. For example, the operation of the SCP is possibly distributed over a range spanning from a single processor to many processors. Another option is to take advantage of interconnected SANs for mutual support, redundancy and security services, thereby profiting from various connection and linking schemes. Furthermore, as a spin-off, the binary zoning approach may be used for not only the booting of arrays of hosts, but also for other purposes.. Rather, the scope of the present invention is defined by the appended claims and includes both combinations and subcombinations of the various features described hereinabove as well as variations and modifications thereof which would occur to persons skilled in the art upon reading the foregoing description.

CLAIMS

1. A method for Storage Area Network (SAN) security comprising booting, the SAN comprising:

physical devices comprising a first array of hosts (1) and a second array of storage devices (4),

a storage network (5') with network links (5),

a users network (6') with users network links (6), and

a SAN Switch (2, 2A) coupled intermediate the first array and the second array and to each physical device via network links and to the users network via a users network link, the SAN Switch routing I/O commands to the physical devices and being configured for accepting zoning commands defining zones for communication between at least one host and at least one storage device,

the method being characterized by comprising the steps of:

operating binary zoning for security comprising default zoning and work zoning permitting the creation of, respectively, at least one default zone and at least one work zone, the binary zoning always first residing in default zoning, and

in default zoning:

mutually isolating each one of the physical devices, and

running a security procedure on each one of the physical devices for legitimacy verification, and

in work zoning:

zoning only legitimate physical devices.

2. The method according to Claim 1, characterized by comprising the steps of:

running, in default zoning, of the security procedure and thereafter,

creating, in work zoning, of at least one work zone comprising at least one legitimate host and at least one legitimate storage device.

3. The method according to Claim 1 or 2, wherein running the security procedure further comprises the steps of:

running an authentication procedure for presence and legitimacy verification of each one host out of the first array, and

an identification procedure for presence and legitimacy verification of each one storage device out of the second array.

4. The method according to Claim 1, or 2, or 3, further comprising the steps of:

running continuously the security procedure for presence and legitimacy verification of the physical devices actually coupled in operation with the SAN, and

rezoning in real time the at least one work zone according to configuration changes associated with running the security procedure continuously.

5. The method according to Claim 3, wherein

a host comprises at least one HBA which is identified by a first WWN (World Wide Number), and

a storage device comprises at least one LU (Logical Unit), and identified by a second WWN and by at least one LUN (Logical Unit Number),

the security procedure being further characterized by comprising the steps of:

authenticating each one host out of the first array independently of the first WWN, and

identifying each one storage device out of the second array by the second WWN and by the at least one LUN.

6. The method according to Claim 1, wherein the SAN further comprises:

a System Administration (SA) workstation coupled to the users network and to the SAN Switch, the SA workstation being configured for managing, securing and booting the SAN, and

the method being further characterized by comprising the steps of:

entering meta-zoning instructions via the SA workstation, the meta-zoning instructions defining programming commands for automatically deriving default zoning and work zoning, and

programming automatically the SAN Switch, according to the meta-zoning instructions, into default zones and work zones.

7. The method according to Claim 6, further characterized by the step of

controlling dynamically the binary zoning of the SAN Switch by entering meta-zoning instructions via the SA workstation.

8. The method according to Claim 6, wherein the SAN further comprises:

at least one HBA in each one host out of the first array, and

the meta-zoning instructions are further characterized by comprising:

instructions for zoning in a work zone at least one HBA pertaining to a legitimate host with at least one legitimate storage device.

9. The method according to Claim 6, wherein the SAN further comprises:

at least one legitimate host out of the first array comprising a plurality of HBAs, and

the meta-zoning instructions are further characterized by comprising:

instructions for zoning in a work zone each one out of the plurality of HBAs comprised in a legitimate host with at least one legitimate storage device.

10. The method according to Claim 1, further comprising the step of:

burning-in the default zones in the SAN Switch, for automatically returning to and always start operation in default zoning, wherein the physical devices are mutually isolated.

11. The method according to Claim 1, wherein

the SAN Switch comprises a plurality of ports, each port out of the plurality of ports having a port identity, and

each one physical device is coupled to at least one port out of the plurality of ports,

the security procedure being further characterized by comprising the step of:

verifying the legitimacy of each one of the physical devices independently of the port identity of the at least one port to which one physical device is coupled.

12. The method according to Claim 11, wherein

the SAN Switch comprises a plurality of ports, for coupling each one physical device to at least one port out of the plurality of ports,

the method being further characterized by

returning immediately the at least one port from which a physical device is decoupled, to a default zone.

13. The method according to Claim 11, further characterized in that

a port out of the plurality of ports of the SAN Switch always resides in a default zone when being coupled to a physical device.

14. A method for Storage Area Network (SAN) booting, the SAN comprising:

physical devices comprising a first array of hosts (1) and a second array of storage devices (4),

a storage network (5') with network links (5),

a users network (6') with users network links (6), and

a SAN Switch (2) coupled intermediate the first array and the second array and to each physical device via network links and to the users network via a users network link, the SAN Switch routing I/O commands to the physical devices and being configured for accepting zoning commands defining zones for communication between at least one host and at least one storage device,

the method being characterized by comprising the steps of:

operating a binary zoning for booting comprising default zoning and work zoning permitting the creation of, respectively, at least one default zone and at least one work zone, the binary zoning always first residing in default zoning, and

in default zoning:

booting the first array of hosts in mutual isolation and starting the second array of storage devices,

verifying operation of the physical devices, and

in the working mode:

zoning only operative physical devices.

15. The method according to the Claims 1 or 14, characterized by comprising the step of:

configuring the storage network as a Fibre Channel network.

16. The method according to the Claims 14 or 15, characterized by comprising the steps of:

running the boot procedure and thereafter,

creating, in work zoning, of at least one work zone comprising at least one operative host and at least one operative storage device.

17. The method according to Claim 14, 15, or 16, further comprising the steps of:

running continuously the booting procedure for presence and operation verification of the physical devices actually coupled in operation with the SAN, and

rezoning in real time the at least one work zone according to configuration changes associated with presence and operation of the physical devices actually coupled to the SAN.

18. The method according to Claim 14, wherein the SAN further comprises:

a System Administration (SA) workstation coupled to the users network and to the SAN Switch, and

the method being further characterized by comprising the steps of:

entering meta-zoning instructions via the SA workstation, the meta-zoning instructions defining default zoning and work zoning, and

programming automatically the SAN Switch into work zones for operative physical devices according to the meta-zoning instructions.

19. The method according to Claim 14, further comprising the step of:

burning-in the default zones in the SAN Switch, for automatically returning to and always start operation in the default zoning, wherein the physical devices are mutually isolated.

20. The method according to Claim 19, wherein

the SAN Switch comprises a plurality of ports, for coupling each one physical device to at least one port out of the plurality of ports,

the method is further characterized by

returning immediately the at least one port from which a physical device is decoupled, to the default zone.

21. The method according to Claim 19, further characterized in that

a port out of the plurality of ports of the SAN Switch always resides in a default zone when being coupled to a physical device.

22. The method according to the Claims 1 or 14, further characterized in that:

the SAN Firewall is packaged with the SAN Switch to form a single unit.

23. The method according to the Claims 1 or 14, further characterized in that:

the SAN Firewall and the SAN Switch are functionally integrated to form a single unit package.

24. The method according to the Claims 1 or 14, further characterized in that:

the SAN Firewall functions operate on a host selected from the first array.

25. The method according to any of the Claims 1 or 14, further characterized in that:
the SAN Firewall functions operate on a remote host coupled to the SAN Switch.

26. The method according to any of the Claims 1 to 14, further characterized in that:
the SAN Firewall functions operate on a remote host coupled to the SAN Switch via a network link coupled to a global communication network.

27. A system for operating SAN security and booting, the system comprising:
physical devices comprising a first array of hosts (1) and a second array of storage devices (4),
a storage network (5') with storage network links (5),
a users network (6') with users network links (6), and
a SAN Switch (2) coupled intermediate the first array and the second array and to each physical device via network links, and coupled to the users network via a users network link, the SAN Switch routing I/O commands to the physical devices and being configured for accepting zoning commands defining zones for communication between at least one host and at least one storage device, the SAN Switch comprising a plurality of ports for coupling each one of the physical devices to at least one port out of the plurality of ports by at least one network link (5),
the system being characterized in that:
a SAN Firewall (3) is coupled by a storage network link to a SAN-Firewall-port (sf) accommodated in the SAN Switch and coupled by a user network link to the users network, the SAN Firewall being configured to automatically program the SAN Switch into zones, with each zone residing in either one of a binary zoning comprising:
in default zoning, at least one default zone counting only two ports, with a first SAN-Firewall-port coupled to the SAN Firewall and connected to a second device-port (h, d) coupled to and isolating a physical device, the SAN Firewall operating at least one security verification procedure on the isolated physical device, and
in work zoning, at least one work zone coupling at least three ports, with a single SAN-Firewall-port (sf), and at least two ports coupling only security verified physical devices counting at least one host port (h), and at least one storage device port (d).

28. The system according to Claim 27, further characterized in that:

the SAN Firewall operates the at least one security and booting procedure in associative operation with the physical devices upon start of the SAN, in default zoning, and

the physical devices failing the at least one security and booting procedure remain isolated in a default zone.

29. The system according to Claim 27, further characterized in that:

the SAN Firewall continuously runs the at least one security and booting procedure in associative operation with the physical devices during operation of the SAN, to update configuration of legitimate physical devices.

30. The system according to Claim 27, or 28, or 29, wherein

the at least one security and booting procedure is a security procedure for securing the SAN, whereby each one host out of the first array is verified for authenticity and each one storage device out of the second array is verified for identity.

31. The system according to Claim 27, further characterized by

default zones being burnt-in in the SAN Switch to always start operation in default zoning.

32. The system according to Claim 31, further characterized by

a port of the SAN Switch from which a physical device is decoupled, immediately returns to a default zone.

33. The system according to Claim 31, further characterized by

a physical device being coupled to a port of the SAN Switch, always couples to a default zone.

34. The system according to Claim 27, further comprising:

a third array of user workstations (7) coupled to the users network and comprising a System Administrator (SA) workstation (8) coupled to the users network and to the SAN Firewall, the SA workstation being configured for managing, securing and booting the SAN, the system being further characterized in that:

meta-zoning instructions, entered at the SA workstation are received at the SAN Firewall where programming commands are derived automatically to zone the SAN Switch in work zones.

35. The system according to Claim 34, further characterized by:

dynamically controlling binary zoning of the SAN Switch by entering meta-zoning instructions via the SA workstation.

36. The system according to Claim 27, wherein

a host comprises at least one HBA (Host Bus Adaptor) which is identified by a first WWN (World Wide Number), and

a storage device comprises at least one LU (Logical Unit) which is identified by a second WWN and by at least one LUN (Logical Unit Number),

the security procedure being further characterized by comprising the steps of:

authenticating each one host out of the first array independently of the first WWN, and

identifying each one storage device out of the second array by the second WWN and by the at least one LUN.

37. The system according to Claim 36, wherein the SAN further comprises:

at least one HBA in each one host out of the first array, and

the meta-zoning instructions are further characterized by comprising:

instructions for zoning in a work zone at least one HBA pertaining to a legitimate host with at least one legitimate storage device.

38. The system according to Claim 36, wherein the SAN further comprises:

at least one legitimate host out of the first array comprising a plurality of HBAs, and

the meta-zoning instructions are further characterized by comprising:

instructions for zoning in a work zone each one out of the plurality of HBAs comprised in a legitimate host with at least one legitimate storage device.

39. The system according to Claim 27, wherein

each port out of the plurality of ports of the SAN Switch has a port identity, and

each one physical device is coupled to at least one port out of the plurality of ports,

the security procedure being further characterized by comprising:

verifying the legitimacy of each one of the physical devices independently of the port identity of the at least one port to which one physical device is coupled.

40. The system according to Claim 27, further characterized in that:
the at least one security and booting procedure is a booting procedure running in the SAN Firewall, as SAN Firewall functions to verify booting of each one host out of the first array and to verify operation of each one storage device out of the second array, allowing simultaneous booting of the first array of hosts in mutual isolation.

41. The system according to Claim 27, further characterized in that:
the SAN Firewall is packaged with the SAN Switch to form a single unit.

42. The system according to Claim 27, further characterized in that:
the SAN Firewall and the SAN Switch are functionally integrated to form a single unit package.

43. The system according to Claim 27, further characterized in that:
the SAN Firewall functions are operated on a host selected from the first array.

44. The system according to Claim 27, further characterized in that:
the SAN Firewall functions are operated on a remote host coupled to the SAN Switch.

45. The system according to Claim 27, further characterized in that:
the SAN Firewall functions are operated on a remote host coupled to the SAN Switch via a network link coupled to a global communication network.

46. A system for SAN booting, the system comprising:
physical devices comprising a first array of hosts (1) and a second array of storage devices (4),
a storage network (5') with storage network links (5),
a users network (6') with users network links (6), and
a SAN Switch (2) coupled intermediate the first array and the second array and to each physical device via network links, and coupled to the users network via a users network link, the SAN Switch routing I/O commands to the physical devices and being configured for accepting zoning commands defining zones for communication between at least one host and

at least one storage device, the SAN Switch comprising a plurality of ports for coupling each one of the physical devices to at least one port out of the plurality of ports by at least one network link (5),

the system being further characterized by

configuring the SAN Switch for default zoning wherein each port out of the plurality of ports for coupling to a physical device is a mutually isolated default zone and the default zoning is burnt-in in the SAN Switch to always start operation in default zoning, whereby the physical device are mutually isolated,

verifying the operation of at least one host of the first array, and

operatively zoning the at least one operative host with at least one storage device.

47. The system according to Claim 1 or 46, wherein

the storage network is preferably a Fibre Channel network.

48. The system according to Claim 46, wherein

the operative state of each host out of the first array is verified automatically.

49. A Security Computer Program (SCP) operating with a SAN for security and booting, the SAN comprising:

physical devices comprising a first array of hosts (1) and a second array of storage devices (4),

a third array of user workstations (7) comprising a System Administrator (SA) workstation (8),

wherein each one host of the first array comprises at least one Host Bus Adaptor (HBA),

a SAN Switch (2, 2A) intermediate the first array and the second array, for routing I/O commands to the physical devices and for accepting zoning commands, the SAN Switch comprising a plurality of ports,

a storage network (5') with network links (5) coupling the SAN Switch to each one of the physical devices and to at least one port out of the plurality of ports by at least one network link (5), the SAN Switch routing I/O commands to the physical devices and being configured for accepting zoning commands defining zones for communication between at least one host and at least one storage device,

a users network (6') with network links (6) coupled to the third array, to the SAN Firewall and to the SAN Switch,

the SCP being characterized by comprising:

at least one SAN Agent and a Firewall Software, both being computer programs operating in mutual association, with an at least one SAN Agent operating in each one host out of the first array, and the Firewall Software operating in the SAN Firewall,

the Firewall Software comprising:

a binary zoning program comprising default zoning and work zoning, for zoning in response to commands derived from meta zoning instructions, comprising defaults zones and work zones wherein:

a default zone operating on two ports only, the first port being a SAN Firewall port (sf) to which the SAN Firewall is coupled and the second port being either one of a host port (h) and a storage device port (d) to which one physical device is coupled, each default zone mutually isolating the physical device, to perform at least one security and booting procedure in isolation, and

a work zone, comprising only physical devices verified by the verification procedure and for coupling at least one host and at least one storage device in associative operation, the default zone comprising at least one host port, one storage device port and the SAN Firewall port.

50. The Security Computer Program according to Claim 49, further characterized by:

in the SAN Agent:

an identity key being sent in periodic repetition to the Firewall Software, and

in the Firewall Software:

a host authentication procedure comprised in the verification procedure for operation with a host identity key received from a SAN Agent, and

a storage device identification procedure comprised in the verification procedure whereby the Firewall Software accesses each one storage device of the second array to check identity parameters comprising a World Wide Name (WWN) and an at least one Logic Unit Number (LUN).

51. The Security Computer Program according to Claim 50, further characterized by:

a security procedure comprising the host authentication procedure and the storage device identification procedure operating in default zoning, and thereafter,

a work zoning procedure for zoning at least one work zone comprising at least one legitimate host and at least one legitimate storage device.

52. The Security Computer Program according to Claim 49, further characterized by:

running continuously the security procedure for presence and legitimacy verification of the physical devices actually coupled in operation with the SAN, and

rezoning in real time the at least one work zone according to configuration changes associated with running the security procedure continuously.

53. The Security Computer Program according to Claim 49, wherein
in default zoning:

an HBA is identified by a first WWN (World Wide Number),

a storage device comprises at least one LU (Logical Unit), and identified by a second WWN and by at least one LUN (Logical Unit Number), and

a list of presence operated and updated by the Firewall Software to record instant configuration of the physical devices coupled to the SAN with identifiers comprising for each host of the first array, a first WWN of an at least one HBA, and for each storage device of the second array, a second WWN and at least one LUN, and port identity coupled to physical devices at the SAN Switch,
the security procedure being further characterized by comprising:
in work zoning:

a status map recording the instant configuration of legitimate physical devices coupled to the SAN with the identifiers, wherein

each one host out of the first array is authenticated independently of the first WWN and of the at least one HBA name, and

each one storage device out of the second array is identified by the second WWN and by the at least one LUN.

54. The Security Computer Program according to Claim 49, wherein

the SA workstation is configured for managing, securing and booting the SAN, and
the SCP is further characterized by comprising:

accepting meta-zoning instructions via the SA workstation, the meta-zoning instructions defining programming commands for automatically deriving default zoning and work zoning, and

programming automatically the SAN Switch, according to the meta-zoning instructions and to the security procedure, into default zones and work zones.

55. The Security Computer Program according to Claim 54, characterized by further comprising:

dynamic control of the SAN by meta-zoning instructions entered via the SA workstation for the binary zoning of the SAN Switch.

56. The Security Computer Program according to Claim 54, wherein the meta-zoning instructions are further characterized by comprising:

instructions for zoning in a work zone at least one HBA pertaining to a legitimate host with at least one legitimate storage device.

57. The Security Computer Program according to Claim 54, wherein

at least one legitimate host out of the first array comprises a plurality of HBAs, and the meta-zoning instructions are further characterized by comprising:

instructions for zoning in a work zone each one out of the plurality of HBAs comprised in a legitimate host with at least one legitimate storage device.

58. The Security Computer Program according to Claim 49, wherein

the SAN Switch comprises a plurality of ports, each port out of the plurality of ports having a port identity, and

each one physical device is coupled to at least one port out of the plurality of ports, the security procedure being further characterized by comprising:

verifying the legitimacy of each one of the physical devices independently of the port identity of the at least one port to which one physical device is coupled.

59. The Security Computer Program according to Claim 49, wherein

the SAN Switch comprises a plurality of ports, for coupling each one physical device to at least one port out of the plurality of ports,

the SCP being further characterized by

returning immediately the at least one port from which a physical device is decoupled to a default zone.

60. The Security Computer Program according to Claim 49, further characterized in that

a port out of the plurality of ports of the SAN Switch always resides in a default zone when being coupled to a physical device.

61. A Security Computer Program operating with a SAN for booting, the SAN comprising:

physical devices comprise a first array of hosts (1) and a second array of storage devices (4),

a storage network (5') with network links (5),

a users network (6') with users network links (6), and

a SAN Switch (2) coupled intermediate the first array and the second array and to each physical device via network links and to the users network via a users network link, the SAN Switch routing I/O commands to the physical devices and being configured for accepting zoning commands defining zones for communication between at least one host and at least one storage device,

the SCP being further characterized by comprising:

operating a binary zoning program for booting comprising default zoning and work zoning permitting the creation of, respectively, at least one default zone and at least one work zone, the binary zoning program always first residing in default zoning, and

in default zoning:

booting the first array of hosts in mutual isolation and starting the second array of storage devices,

verifying operation of the physical devices, and

in the work mode:

zoning only operative physical devices.

62. The Security Computer Program according to the Claims 49 or 61, further characterized by

a SCP configuration adapted for operation on a Fibre Channel network.

63. The Security Computer Program according to Claim 61, further characterized by

the boot procedure operating first, and

at least one work zone comprising at least one operative host and at least one operative storage device being created thereafter in work zoning.

64. The Security Computer Program according to Claim 61, further characterized in that

the booting procedure is operated continuously for presence and operation verification of the physical devices actually coupled in operation with the SAN, and

the at least one work zone is rezoned in real time according to configuration changes associated with presence and operation of the physical devices actually coupled to the SAN.

65. The SCP according to Claims 49 or 61, further characterized by comprising:

a listing procedure for listing the physical devices coupled to the SAN Switch,

a status map procedure for building and maintaining a Status Map recording the legitimate physical devices coupled to the SAN Switch, and

a work zone procedure for commanding automatic zoning of legitimate physical devices recorded in the Status Map.

66. The SCP according to Claim 65, further characterized by comprising:

an update procedure for continuously updating the Status Map in accordance with a configuration of the physical devices coupled to the SAN Switch and with the meta zoning instructions.

67. The SCP according to Claims 61, further comprising:

a System Administration (SA) workstation coupled to the users network and to the SAN Switch, and

the SCP being further characterized by comprising:

entering meta-zoning instructions via the SA workstation, the meta-zoning instructions defining default zoning and work zoning, and

programming automatically the SAN Switch into work zones comprising operative physical devices according to the meta-zoning instructions.

68. The SCP according to Claims 49 or 61, further characterized by:

the Firewall Software being configured to operate on the SAN Firewall when packaged with the SAN Switch to form a single unit.

69. The SCP according to Claims 49 or 61, further characterized by:

the Firewall Software being configured to operate on the SAN Firewall and the SAN Switch when functionally integrated to form a single unit package.

70. The SCP according to Claims 49 or 61, further characterized by:

the Firewall Software being configured to operate on a host selected from the first array.

71. The SCP according to Claims 49 or 61, further characterized by:

the Firewall Software being configured to operate on a remote host coupled to the SAN Switch.

72. The SCP according to Claims 49 or 61, further characterized by:

the Firewall Software being configured to operate on a remote host coupled to the SAN Switch via a network link coupled to a global communication network.

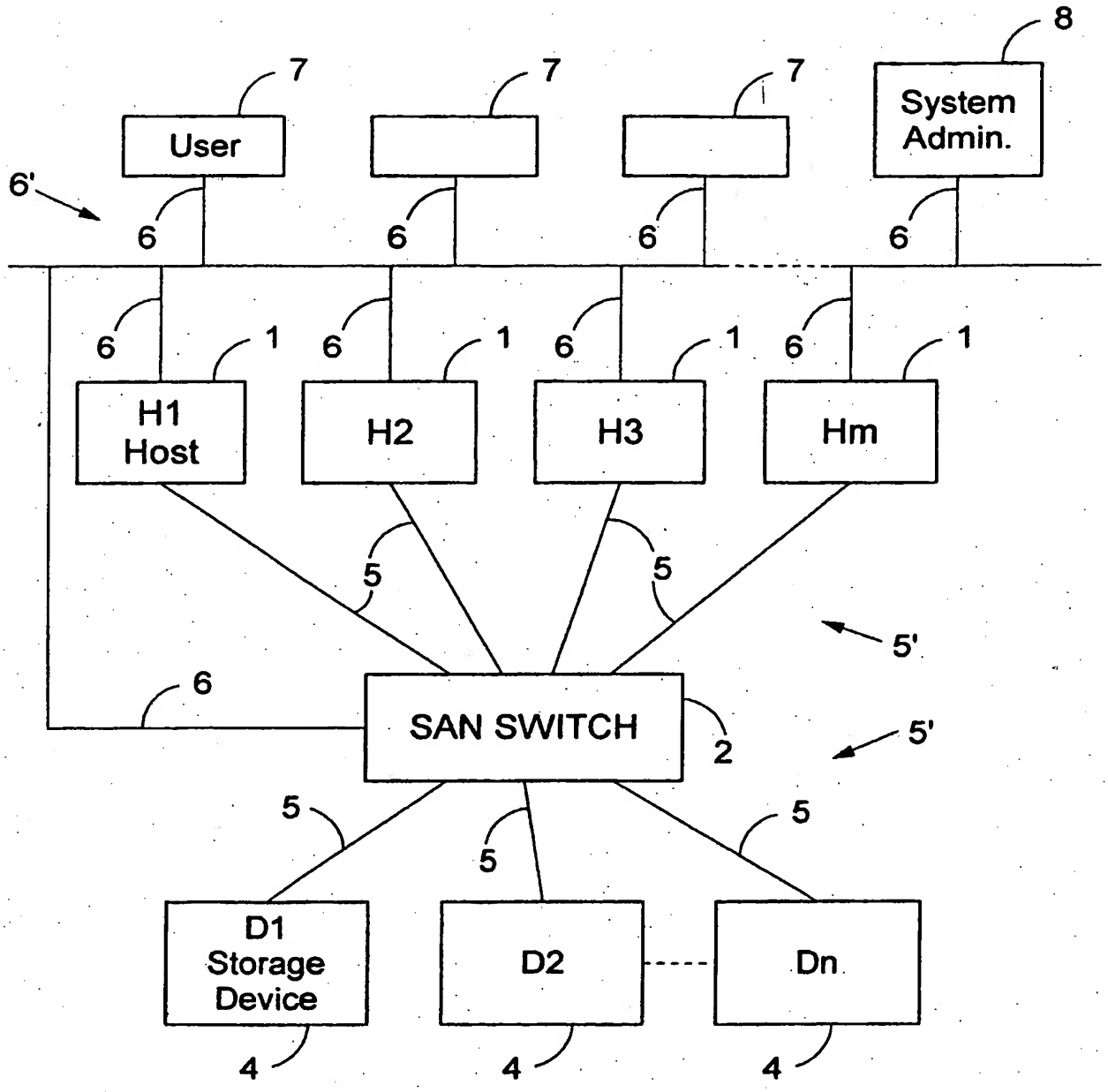


FIG.1 Prior Art

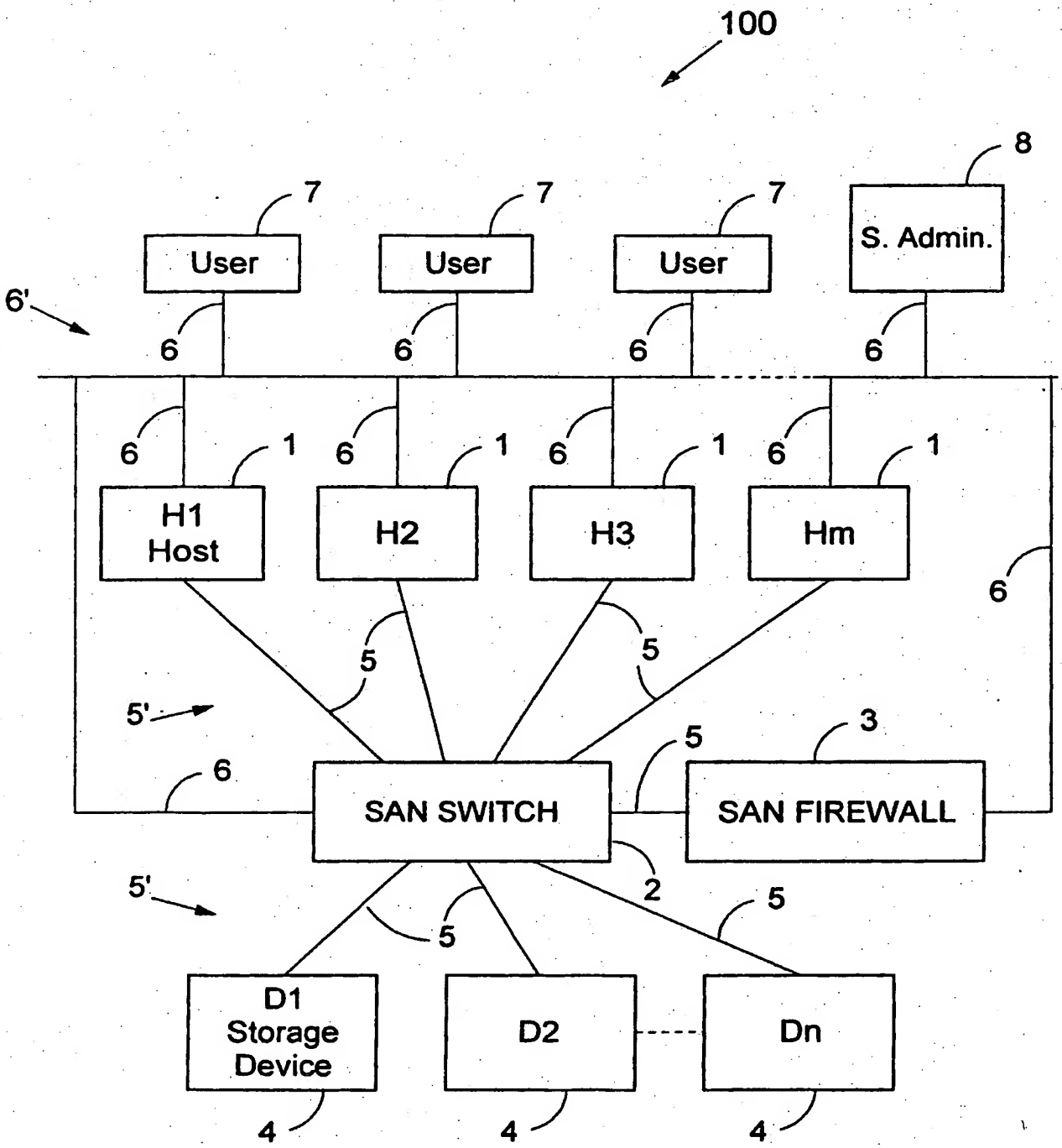


FIG.2

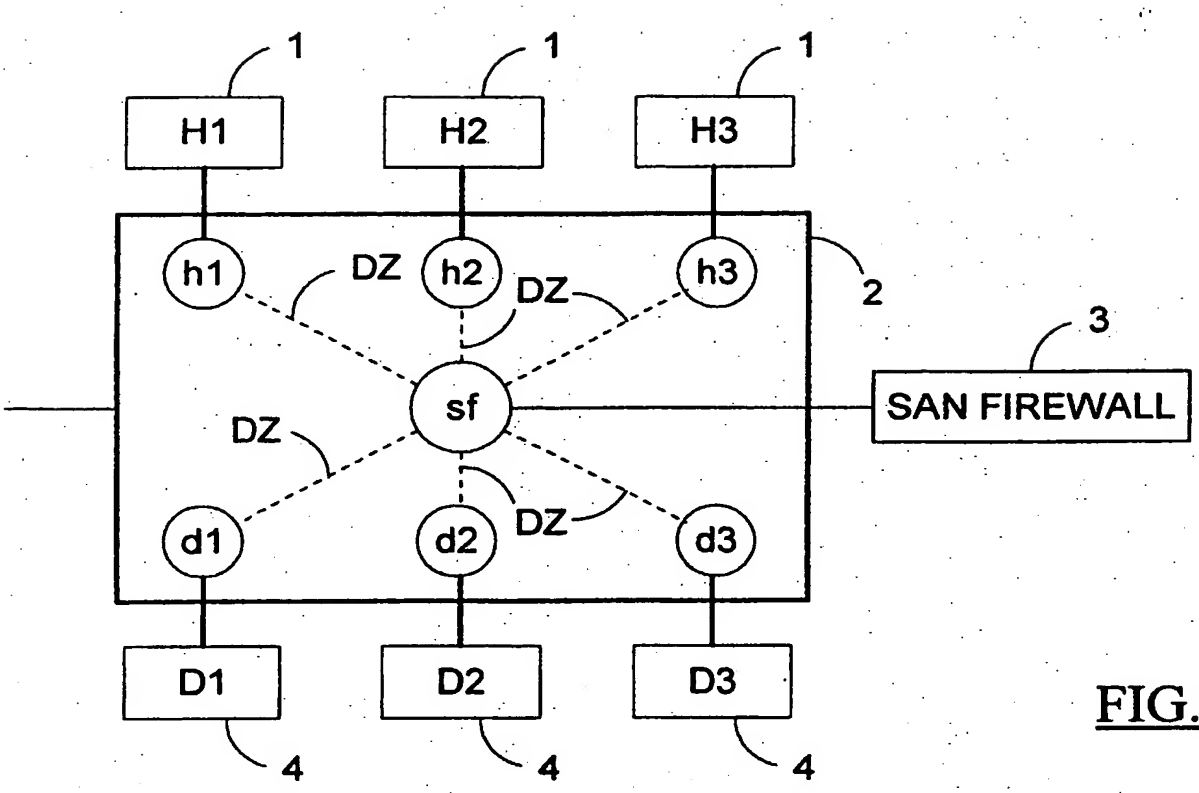


FIG.3

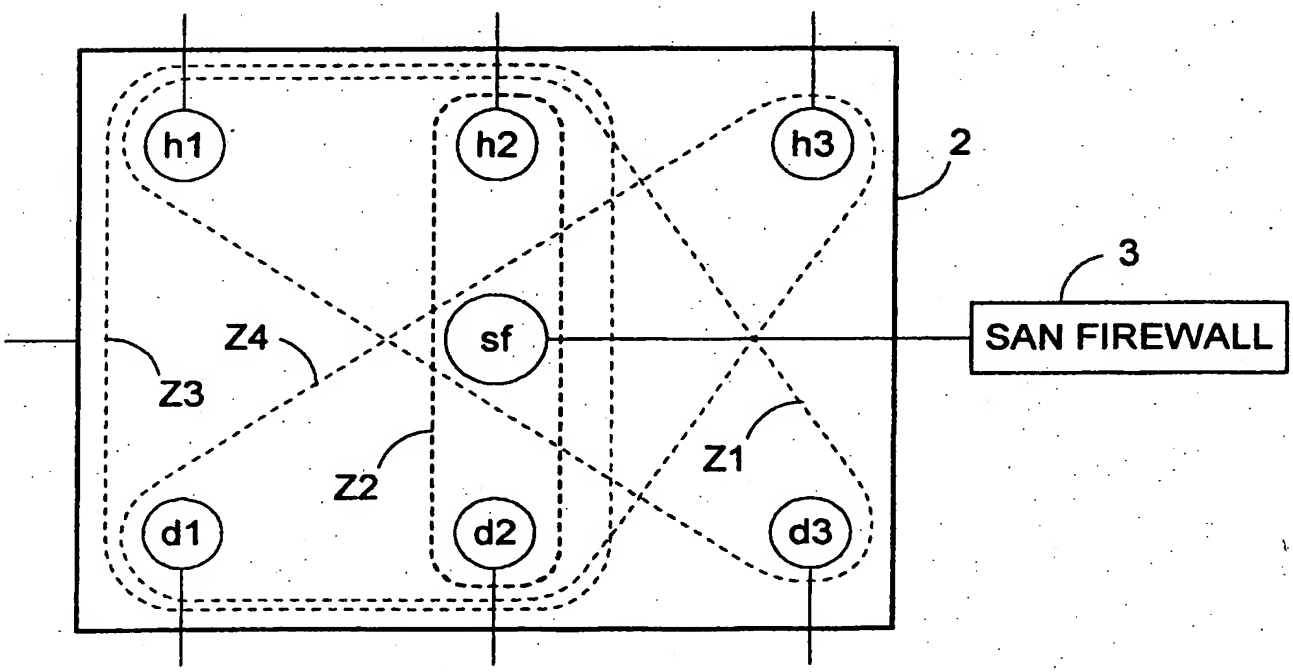


FIG.4

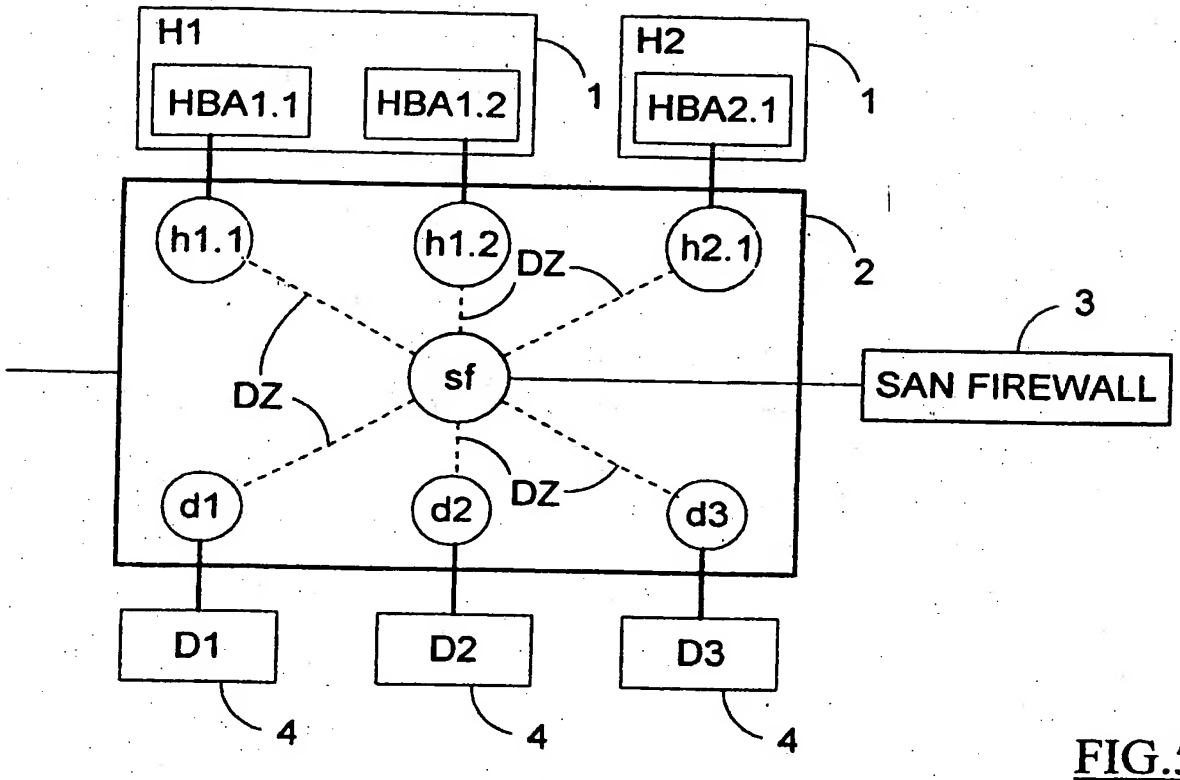


FIG.5

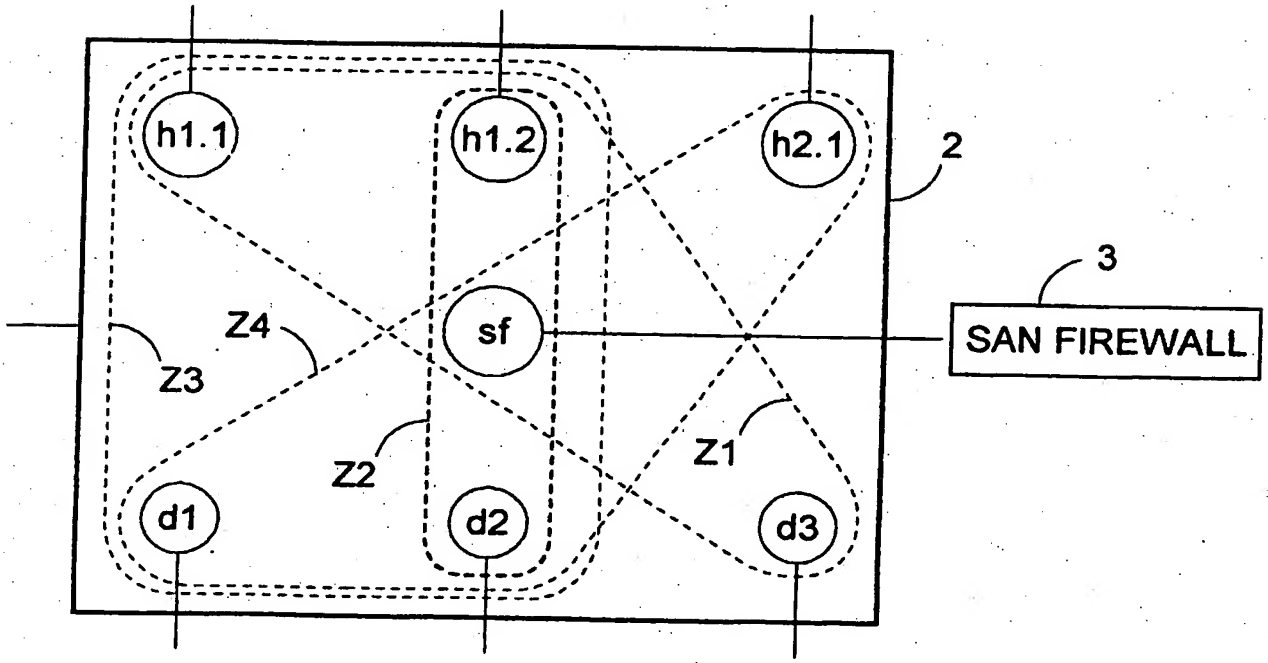


FIG.6

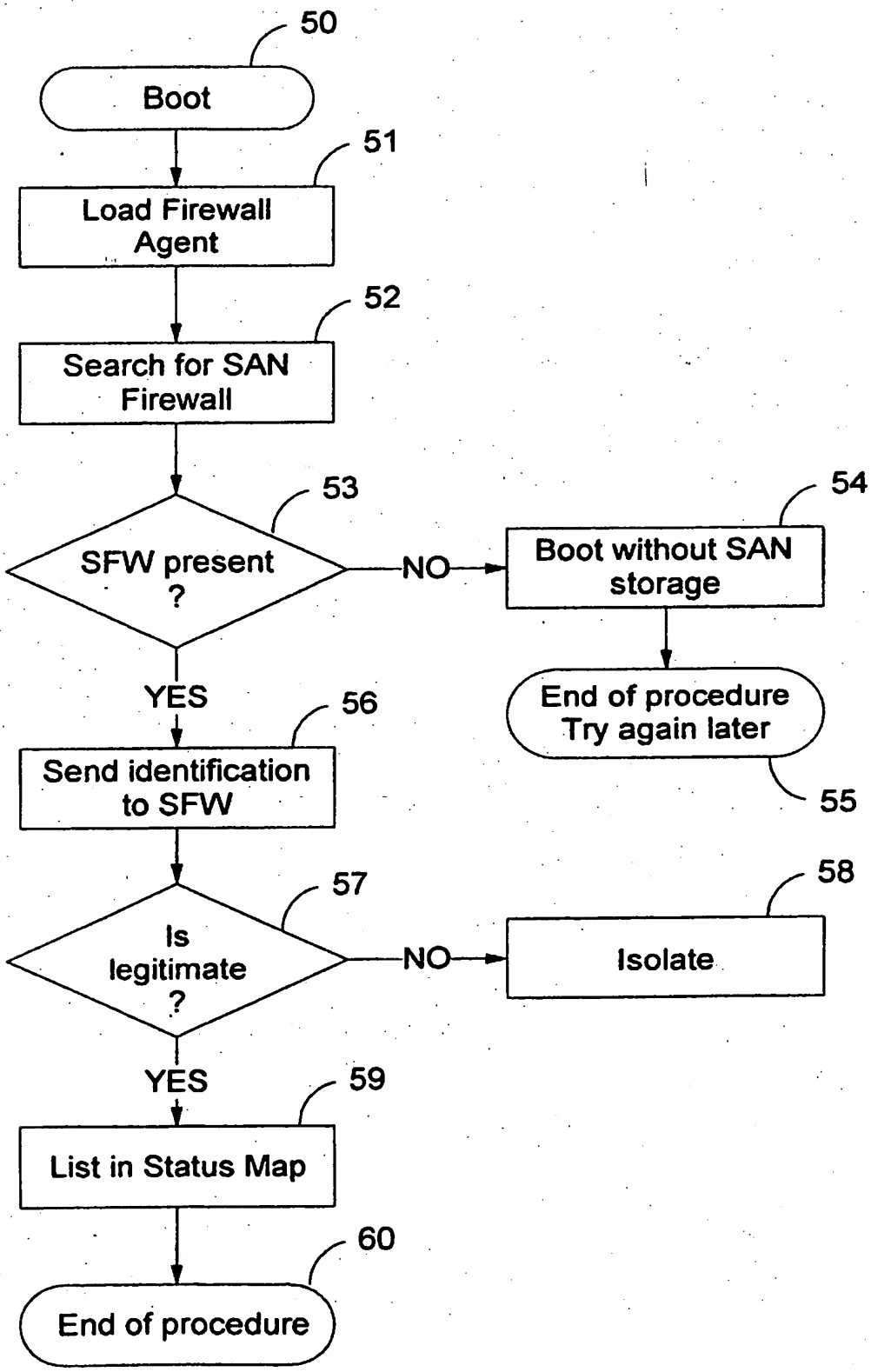


FIG.7

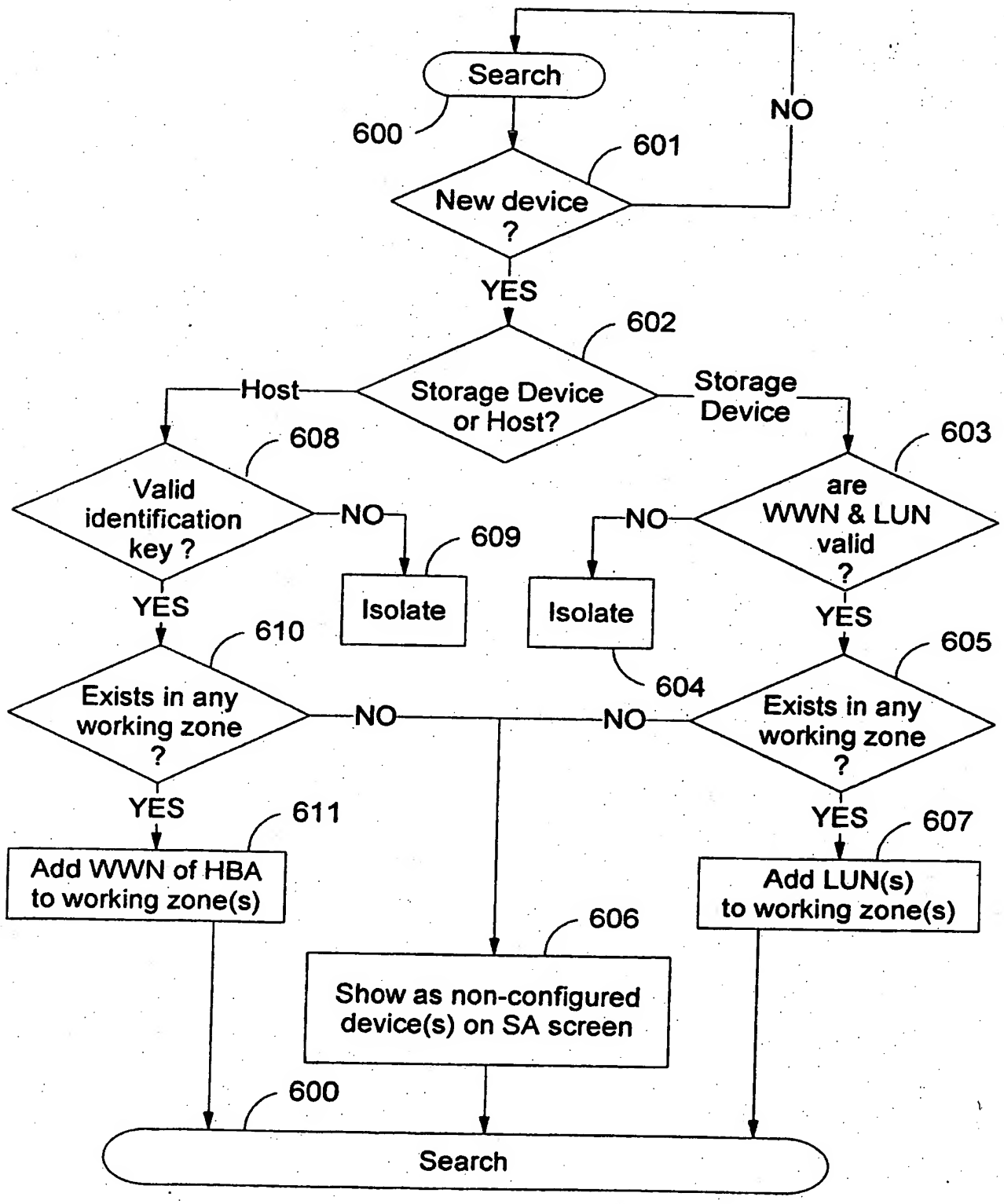


FIG.8

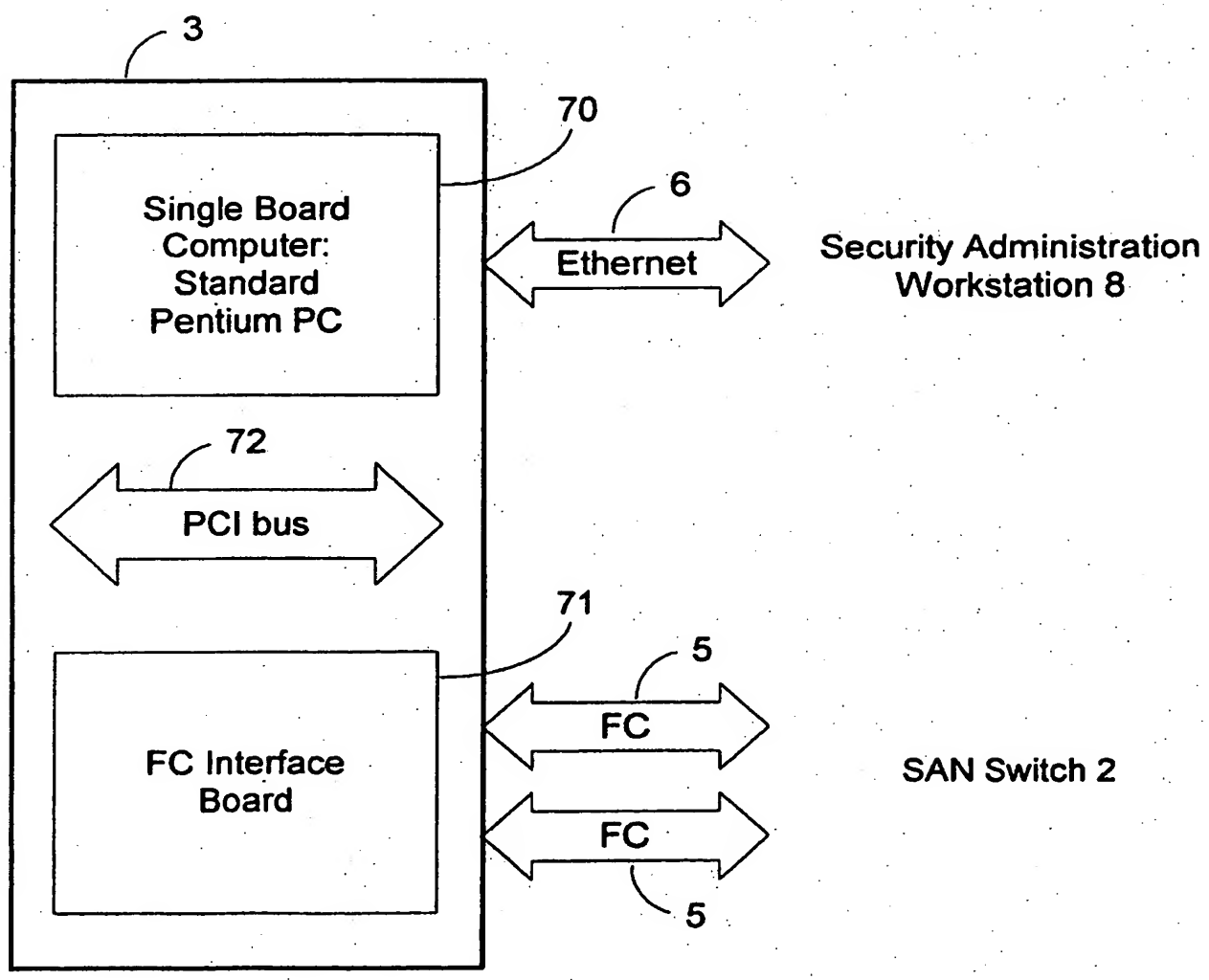

3
70
Single Board Computer: Standard Pentium PC
6
Ethernet
Security Administration Workstation 8
72
PCI bus
71
5
FC
FC Interface Board
SAN Switch 2
FC
5

FIG.9

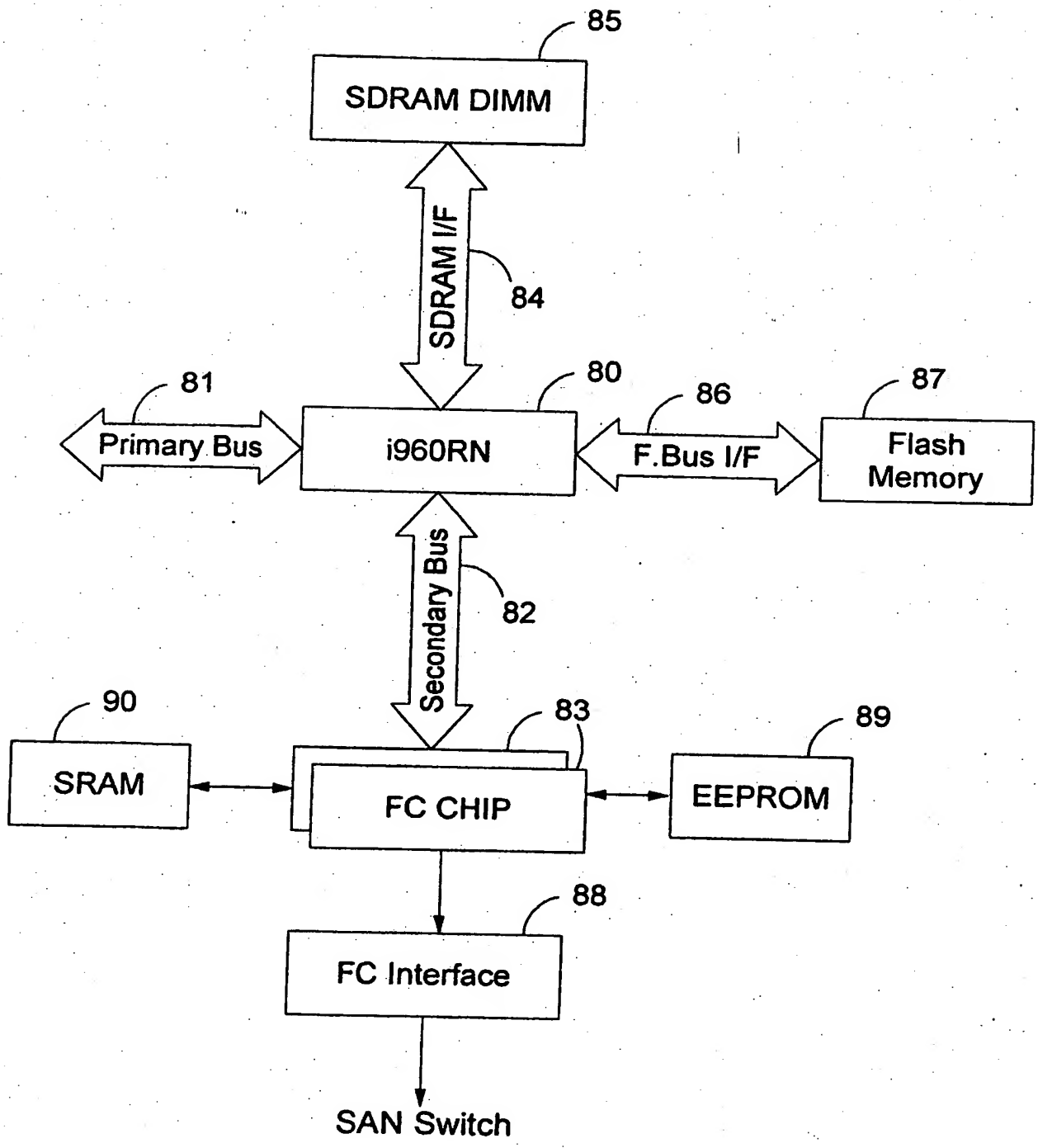


FIG.10

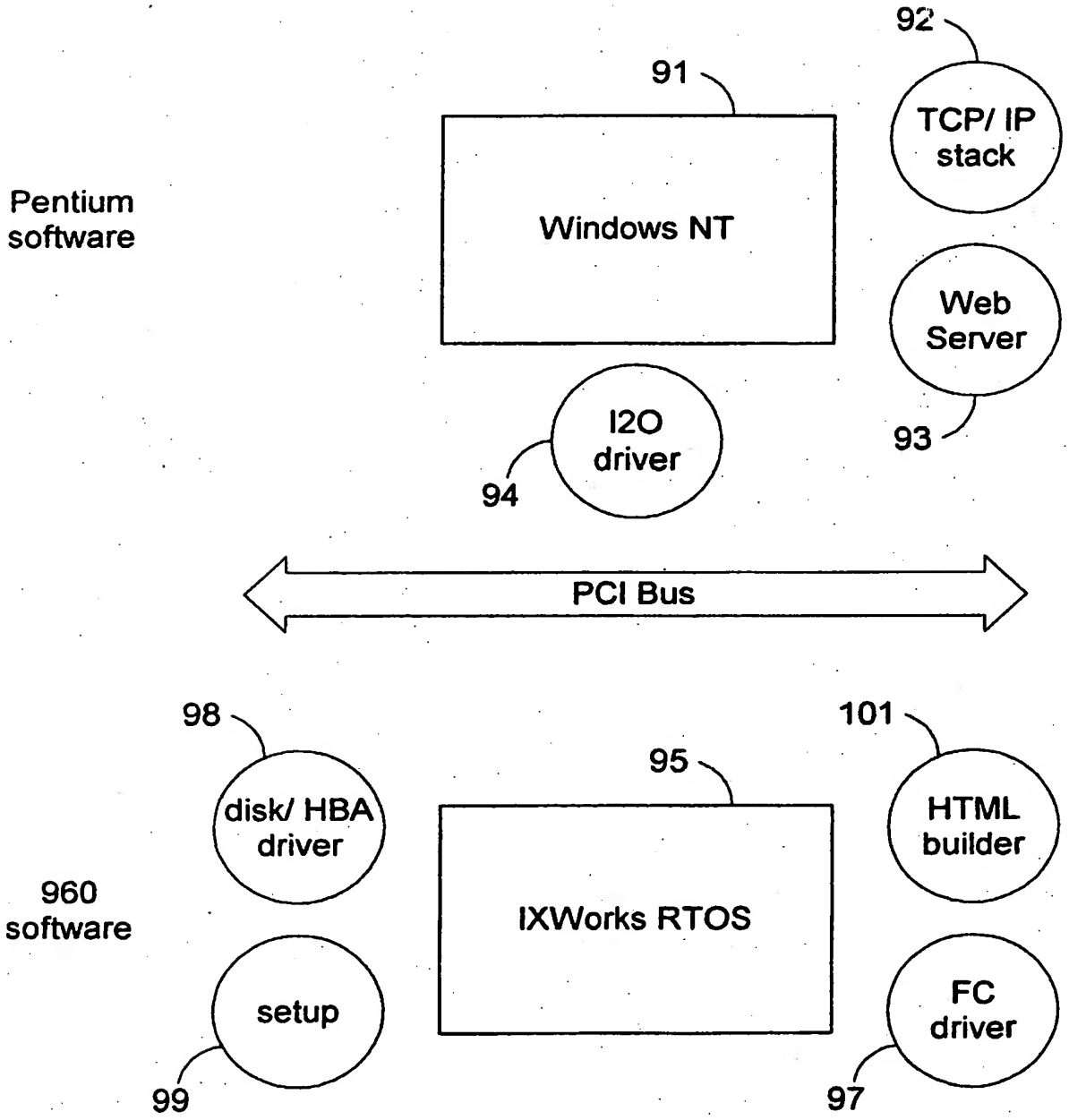


FIG.11

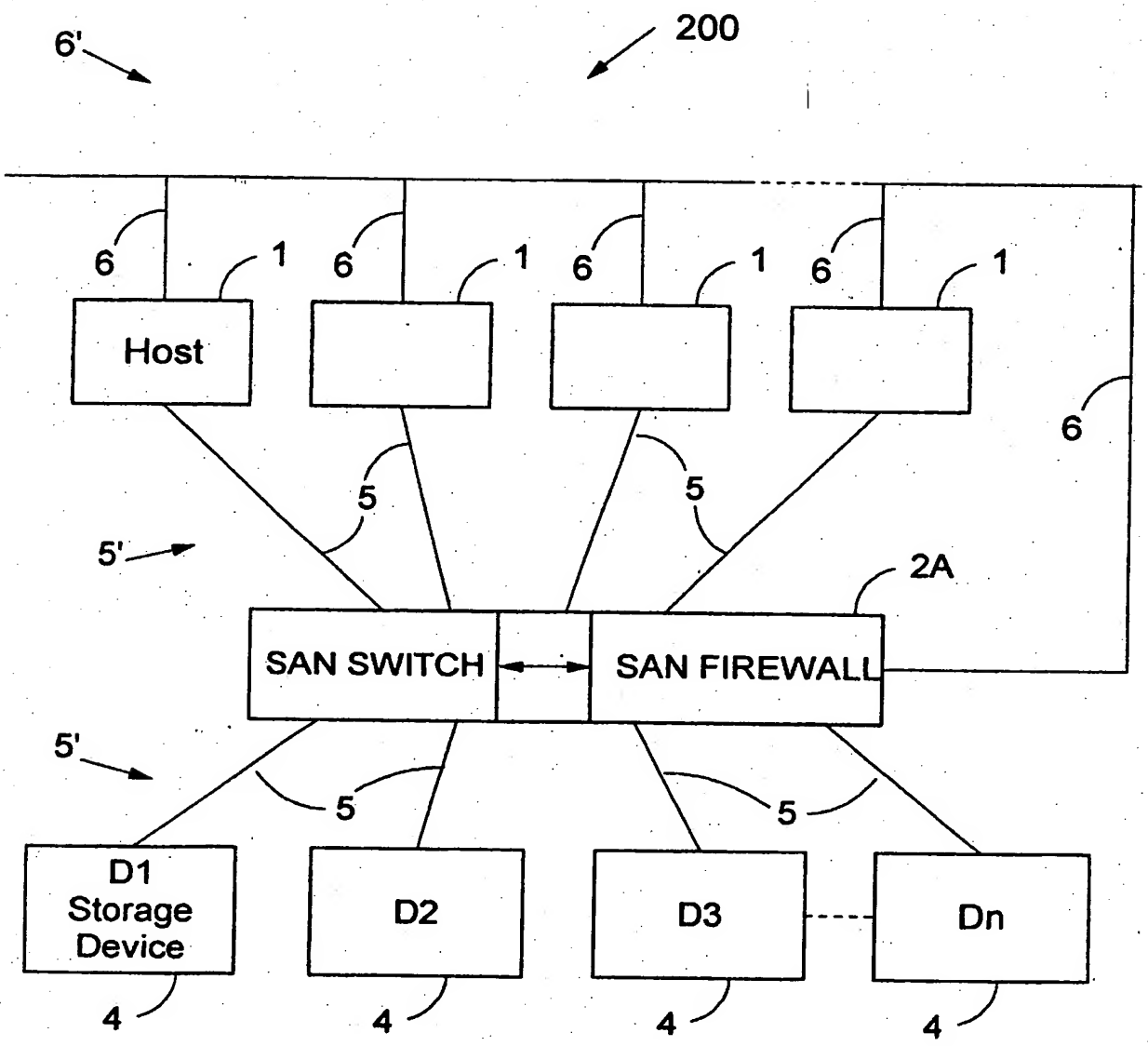


FIG.12

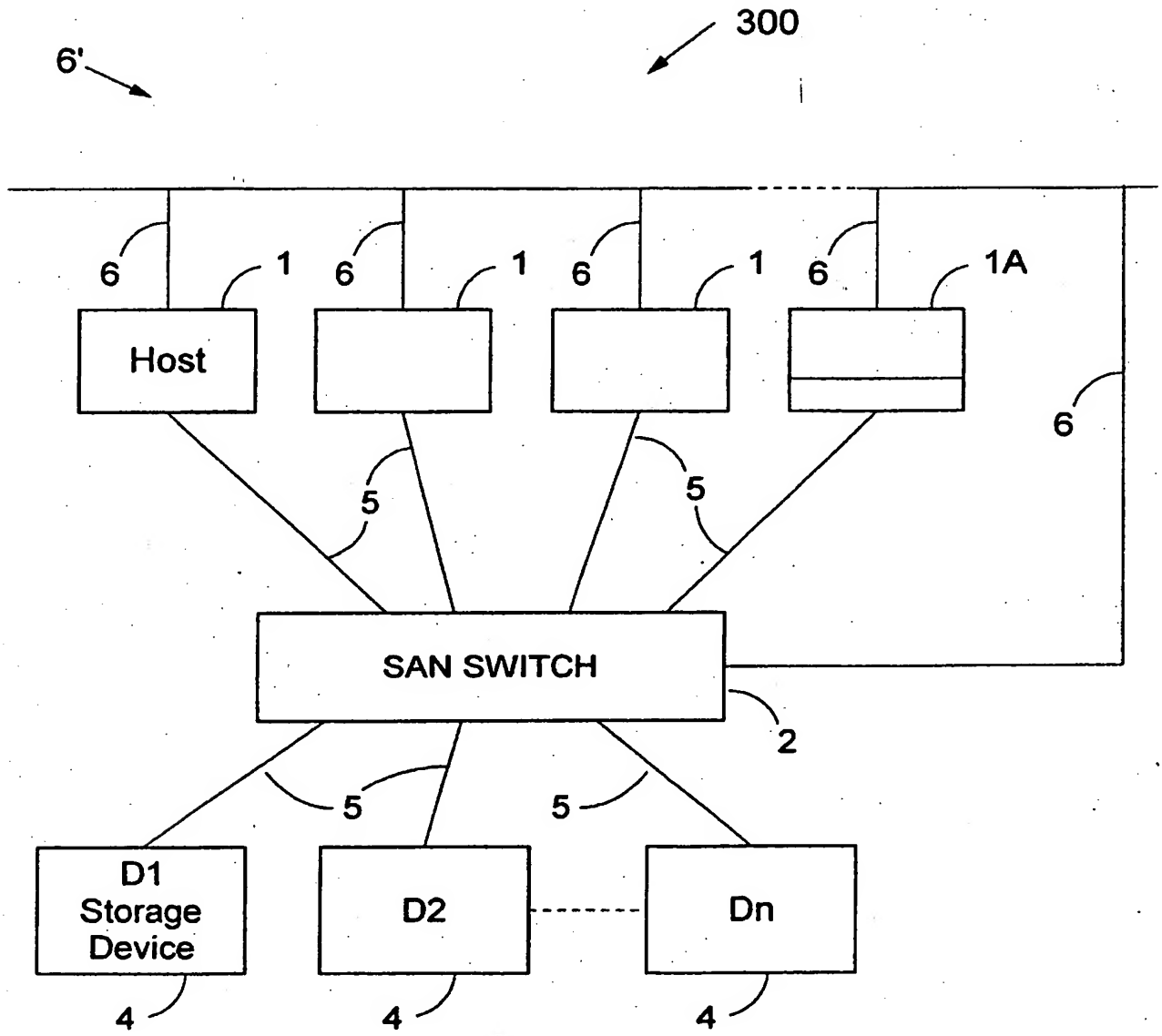


FIG.13

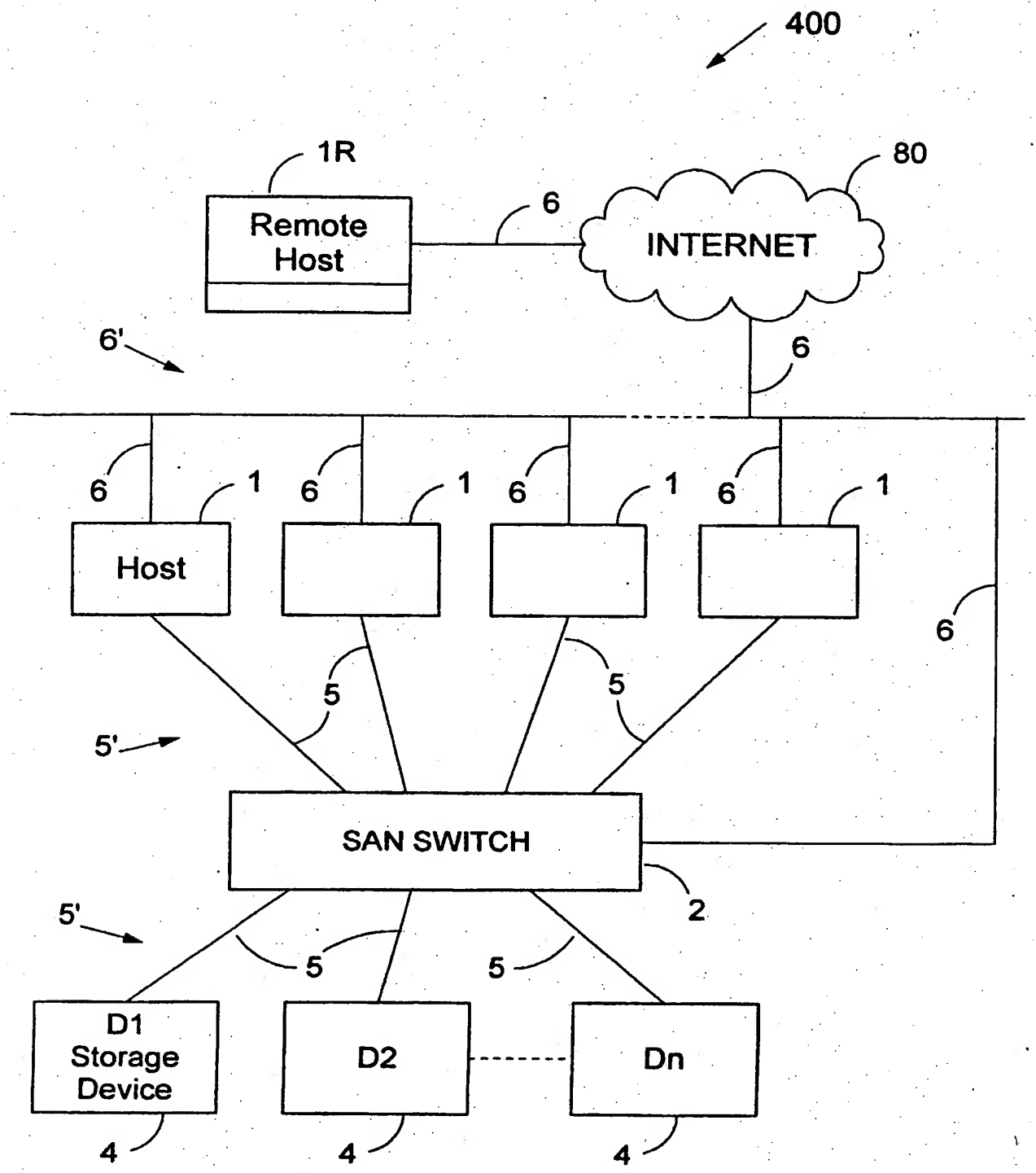


FIG.14

INTERNATIONAL SEARCH REPORT

International Application No.
PCT/IL02/00152

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) :Please See Extra Sheet.
US CL :713/200, 201; 711/163, 164; 709/223, 225, 227, 228, 230
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 713/200, 201; 711/163, 164; 709/223, 225, 227, 228, 230

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

Please See Extra Sheet.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 6,182,226 B1 (REID et al) 30 January 2001, see entire document	1-72
A	US 6,195,366 B1 (KAYASHIMA et al) 27 February 2001, see entire document	1-72
A	US 5,968,176 A (NESSETT et al) 19 October 1999, see entire document	1-72

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 30 JUNE 2002	Date of mailing of the international search report 05 AUG 2002
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer GAIL HAYES Telephone No. (703) 305-9618

Form PCT/ISA/210 (second sheet) (July 1998)★

INTERNATIONAL SEARCH REPORT

Internatio[illegible]lication No.
PCT/IL02/00152

A. CLASSIFICATION OF SUBJECT MATTER:
IPC (7):

G06F 11/30, 12/00, 12/14, 12/16, 13/00, 13/28, 15/16, 15/173; H04L 9/00, 9/32

B. FIELDS SEARCHED
Electronic data bases consulted (Name of data base and where practicable terms used):

BRS (FILES: USPAT, EPO, JPO, IBM TDB'S, US PGPUBS, DERWENT), DIALOG (FILES: COMPSCI, ELECTRON, SOFTWARE)

search terms: network, ethernet, lan, wan, internet, switch, switched, switching, region, zone, zoned, zoning, area, section, sectional, sectioning, sectioned, device, node, component, computer, client, server, terminal, workstation, storage, database, firewall, proxy, restrict, restriction, restricted, restricting, grant, granting, granted, limit, limiting, limited, limitation, rule, right, privilege, condition, communicate, communication, communicating, communicated, transmission, transmit, transmitting, transmitted